

# Advanced Insider Threat Mitigation Workshop Instructional Materials

---

Philip Gibbs/Brookhaven National Laboratory  
Robert Larsen/Los Alamos National Laboratory  
Mike O'Brien/Lawrence Livermore National Laboratory  
Tom Edmunds/Lawrence Livermore National Laboratory

November 2008

**BNL-106047-2008-IR**

**BROOKHAVEN**  
NATIONAL LABORATORY

*a passion for discovery*



U.S. DEPARTMENT OF  
**ENERGY**

Office of  
Science



BNL-106047-2008-IR

*Advanced Insider Threat Mitigation Workshop Instructional Materials*

Philip Gibbs  
Brookhaven National Laboratory

Robert Larsen  
Los Alamos National Laboratory

Mike O'Brien  
Lawrence Livermore National Laboratory

Tom Edmunds  
Lawrence Livermore National Laboratory

November 2008

**Nonproliferation and National Security Department  
Brookhaven National Laboratory**

**U.S. Department of Energy  
National Nuclear Security Administration  
Office of International Material Protection and Cooperation**

## **DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or any third party's use or the results of such use of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof or its contractors or subcontractors. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Notice: This manuscript has been authored by employees of Brookhaven Science Associates, LLC under Contract No. DE-AC02-98CH10886 with the U.S. Department of Energy. The publisher by accepting the manuscript for publication acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

## **Executive Summary**

Insiders represent a formidable threat to nuclear facilities. This set of workshop materials covers methodologies to analyze and approaches to mitigate the threat of an insider attempting abrupt and protracted theft of nuclear materials. This particular set of materials is an update of a January 2008 version to add increased emphasis on Material Control and Accounting and its role with respect to protracted insider nuclear material theft scenarios.

This report is a compilation of workshop materials consisting of lectures on technical and administrative measures used in Physical Protection (PP) and Material Control and Accounting (MC&A) and methods for analyzing their effectiveness against a postulated insider threat. The postulated threat includes both abrupt and protracted theft scenarios.

Presentation is envisioned to be through classroom instruction and discussion. Several practical and group exercises are included for demonstration and application of the analysis approach contained in the lecture/discussion sessions as applied to a hypothetical nuclear facility.

### **Mode of Instruction**

The suggested mode of instruction for these materials is lecture, demonstrations, and small group exercises.

### **Participants**

Participants attending this workshop should currently, or in the near future, be responsible for designing and/or analyzing PP or MC&A systems. It is suggested that the ideal participant pool consist of a mix of PP, MC&A, and vulnerability assessment (VA) professionals.

**Workshop length** – 6-8 training days

# **Insider Threat Identification and Mitigation (ITIM) Workshop Primer**



**Beijing, The People's Republic of  
China**

**February, 2009**

# PRIMER FOR THE ITIM Workshop

## January 2009

### Introduction

This primer is intended to assist **Insider Threat Identification and Mitigation (ITIM) Workshop** students in their understanding of basic principles of physical protection and material control and accounting. While these operational activities seemingly operate separately, they are actually closely integrated in an insider protection system.

Students should be aware that while effective material control and accounting functions play significant roles in an insider protection system, key functions of physical protection are also integral to an insider protection system. Specifically, functions associated with material control activities aid in timely detection and assessment.

Detection and assessment are the main attributes necessary when evaluating overall Material Protection Control and Accounting (MPC&A) system effectiveness against insider threats.

The U.S. Department of Energy (DOE) requires that an insider analysis be conducted consistent with current Design Basis Threat guidance and as part of a site's integrated vulnerability analyses. The analysis is validated on an annual basis. The requirement for conducting an insider analysis appears in regulatory guidance pertaining to Safeguards and Security Programs, Physical Protection, and Material Control and Accounting. It is the responsibility of the site to conduct the analysis and the responsibility of the local DOE office to validate the analysis. Validation is generally done concurrently with approval of a Site Safeguards and Security Plan, during annual surveys conducted by the local DOE office, and during periodic independent inspections conducted by DOE Headquarters.

Routine functions of DOE oversight activities aid in overall insider threat protection. In addition to DOE surveys and inspections, routine and periodic assurance activities required by safety directives support insider protection detection functions and serve to deter potential insiders.

Each section of this primer will highlight the basic MPC&A functions and terminology which will be used in the ITIM Course.

# PRIMER FOR THE ITIM Workshop

## January 2009

### Basic Physical Protection Systems (PPS)

#### Background

Physical protection systems at different sites are seldom identical because of the differences in facilities, targets, and threats. The basic design for physical protection systems is quite well established but considerable engineering and design tailoring is usually required for each site. DOE and NNSA sites use DOE Order 470.4-2. This Manual establishes requirements for the physical protection of safeguards and security (S&S) interests.

#### Objectives

The objectives of the physical protections system should be:

- a. To establish conditions which would minimize the possibilities for unauthorized removal of nuclear material and/or for sabotage ; and
- b. To provide information and technical assistance in support of rapid and comprehensive measures to locate and recover missing nuclear material and to cooperate with safety authorities in minimizing the radiological consequences of sabotage.

#### PPS Functions: Detection, Delay, and Response

An effective physical protection system integrates people, equipment, and procedures for the protection of assets or facilities against theft, sabotage, or other malevolent human attacks. Depending on the assets and possible targets in the facility, a probable type of adversary may be identified. Adversaries can be categorized into three main groups: outsiders, insiders, and outsiders working in collusion with insiders. *Outsiders* include terrorists, criminals, extremists, and hackers. An *insider* is considered anyone with knowledge of operations in the facility and who has unescorted access to security areas and sensitive information. An outsider that operates with insider assistance represents a great challenge for the security system since the insider can move around the facility without raising suspicion and can choose the best time to act. Regardless of these possibilities, the PPS must respond to the challenge and prevent an attack by bringing into effect its three main functions: detection, delay, and response.

#### The Detection Function

Detection is the discovery of an adversary action. It includes sensing of covert or overt intrusion activities. The following is a typical detection sequence:

1. A sensor reacts to a stimulus and initiates an alarm.
  2. The information from the sensor is reported and displayed.
  3. A person assesses the information and judges the alarm to be valid or invalid.
- (Note: detection without assessment is not considered detection.)

An increasing number of exterior and interior sensors for intrusion detection are in the market today. They are designed to respond to specific stimuli and are

## PRIMER FOR THE ITIM Workshop

### January 2009

classified according to whether they are active or passive, covert or visible, volumetric or line detection, line-of-sight or terrain following, and according to application modes. Some are associated with fences, others are buried, and others are freestanding such as infrared sensors and video motion detectors. All sensors are susceptible of generating invalid alarms, called nuisance alarms, which are caused by anything other than an intrusion. Invalid alarms caused by faulty equipment are called false alarms. Some sensors are of the type called dual technology because they respond to two different stimuli thereby reducing the probability of generating nuisance alarms. In interior environments, detection of moving objects or persons plays a very important role in physical security. Most common types are infrared and microwave sensors. For detection of entry through doors or windows, the most common types are electromechanical sensors such as magnetic switches and vibration detectors. Protection of large metallic objects is commonly done through proximity sensors where the metallic object itself becomes part of the detection system. Assessment of alarms is normally done with video cameras strategically located around the facility and aimed to probable targets. Additionally, video cameras can also be effectively used as motion sensors, in which case they are called video motion detectors, or VMDs. They can only be used as sensors, however, in places where there is no movement of objects or persons, such as in storage rooms or vaults. *Entry control* is also included in the detection function. It allows the entry and movement of authorized persons and materials and detects any attempt of unauthorized entry. There are many different technologies for entry control of personnel, but in essence, an entry control system verifies if the person trying to gain access into a facility is in reality who they claim they are. This is based on whether the person has a valid credential, or knows a valid personal identification number, or possesses the proper unique physical characteristic that matches the one on record. In other words, verification is done based on what you have, what you know, or what you are. Examples of credentials include photo ID badge, magnetic card, bar code card, and proximity card, with the last one being among the most secure credential systems these days. In increasing use recently, *biometric* identification systems make use of unique physical characteristics such as fingerprints, hand geometry, retinal pattern, speech recognition, and handwriting. Fingerprinting has been in use for many years and is considered one of the most reliable means of distinguishing one individual from another. With modern technology based on image processing and pattern recognition, automatic fingerprinting is now a common means for entry control. Another example of advanced technology is the retinal scan device, which recognizes the unique pattern of blood vessels in the retina of the eye.

### The Delay Function

## PRIMER FOR THE ITIM Workshop

### January 2009

This function provides elements of delay that slow down adversary progress. Delaying an adversary is an effective means of giving the response force adequate time to respond and interrupt the adversary. Delay elements are normally barriers in the form of fences, barbed concertina tape, reinforced walls and doors, cages around storage bins, heavy duty roll-up doors, to mention a few. Overall PPS effectiveness can be increased by placing sensors at delay points, preferably in a way that delay takes place right after detection to improve the assessment function. Delay before detection can only be a deterrent and not an effective measure because it does not provide additional time to respond to the adversary. Delay elements outside the facility, such as big boulders, trees and shrubbery, could force adversaries to change or abandon their tactic. Conventional construction is relatively weak for a highly motivated and well-trained attacker. Chain-link fences can only stop small vehicles but are totally ineffective against medium and large trucks. However, if an adversary encounters a series of progressively more difficult barriers, he will be forced to carry heavier equipment and tools that will contribute to increase the delay time. In any event, the most cost-effective means of improving the delay provided by a chain-link fence against climbing is to add a roll of BTC to the outriggers. Other forms of delay elements include reinforced concrete walls, special doors and windows, reinforced roofs and floors, and dispensable barriers. *Dispensable barriers* are those that are deployed only when necessary, that is, during an attack. They are normally foams or other chemical products that can delay or even totally immobilize an intruder. Due to their high cost, they are more appropriate to use near the asset to be protected, preferably in a closed area to contain the collateral contamination and reduce the clean up task.

### **The Response Function**

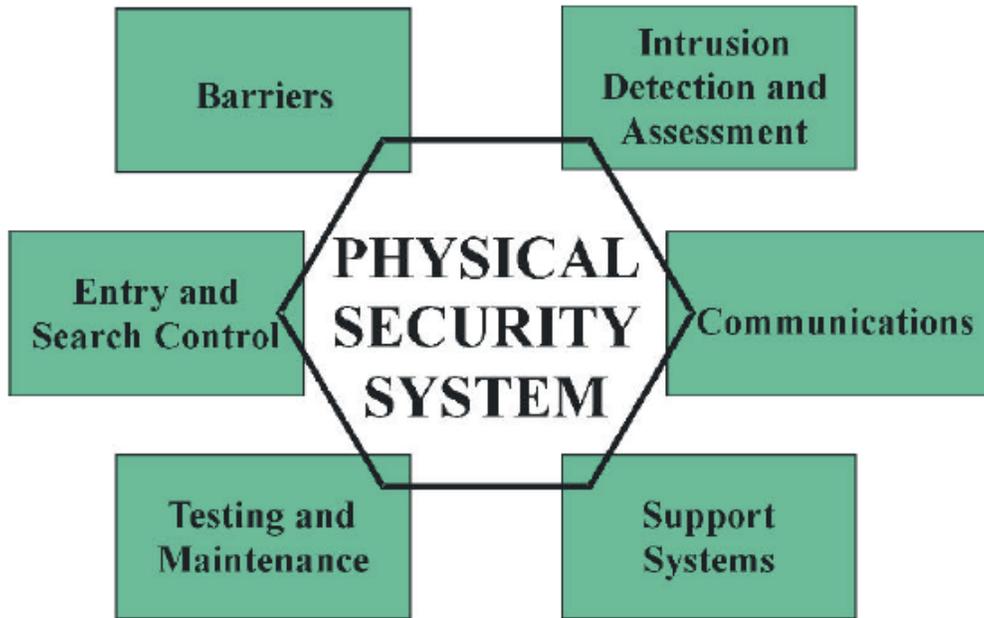
The response function consists of the actions taken by the response force to prevent adversary success and includes: responding personnel, contingency planning, communication, and interruption. Responding personnel may include proprietary or contract guards, local and state police, and in some cases federal agencies such as the FBI, DEA, or Customs. *Contingency planning* is the development of well-documented procedures for identifying potential targets, respond to different threats, interact with outside agencies, and determine what level of force guards can use in different situations. Once potential targets are identified, security personnel can evaluate likely adversary routes and develop tactical plans to address various threats to the facility and to determine guard patrol routes and schedules. Procedures and plans for guard actions in the event of an adversary attack should be well established and practiced through periodic training exercises. If outside agencies are likely to participate in the response, joint training exercises should be planned and executed. *Communication* is a vital component of the response function since all other system functions depend heavily on proper communication between all responding personnel. Information must be transferred through this network with speed and accuracy.

## PRIMER FOR THE ITIM Workshop January 2009

Communication to the response force must contain information about adversary actions and instructions for deployment. The most common means of communication to the response force is through clear-voice radios, normally of the FM (frequency modulation) type. Clear voice means that the signal has not been encrypted or encoded. As a result, however, *eavesdropping* on the part of adversaries is possible through the use of standard receivers or scanners. If an adversary can monitor a conventional radio transmission, they can also transmit *deceptive* messages with a conventional transmitter tuned to the same channel frequency. Another form of disturbing a radio transmission, known as *jamming*, can be done by inserting an unwanted signal into the channel that can mask a desired signal. If the jamming signal is of sufficient power, it can totally destroy the true signal making it unusable. Periodic jamming exercises should be established to practice procedures to counteract a jamming attack. Alternate means of communication, such as intercoms, public address, or cellular phones must be available at all times and everybody in the response force must know what to do in case of a jamming attack. One modern technology for counteracting eavesdropping, deception and jamming is the spread spectrum or frequency-hopping communication system. In this system, the master transmitter makes the other receivers to follow it automatically from channel to channel as the message is transmitted. For any particular receiver in the system, the message is received like any other continuous message. For an intruder, however, the transmission is going to sound like bits and pieces making impossible the intelligibility of the message. The last segment of the response function is *interruption*, which is defined as the successful arrival in sufficient number of the response force at an appropriate location to confront the adversary. The probability of successful interruption can be enhanced by the use of deployment through known, protected paths. To measure the effectiveness of a PPS, a procedure called *timely detection* can be performed to obtain the probability of interruption based on cumulative delays and probabilities of detection along adversary paths. Timely detection consists in obtaining a cumulative probability of detection at a point in time and place where the remaining adversary time just exceeds the guard response time. In other words, at a point where there is still enough time left for the response force to interrupt the adversaries before their goal is completed.

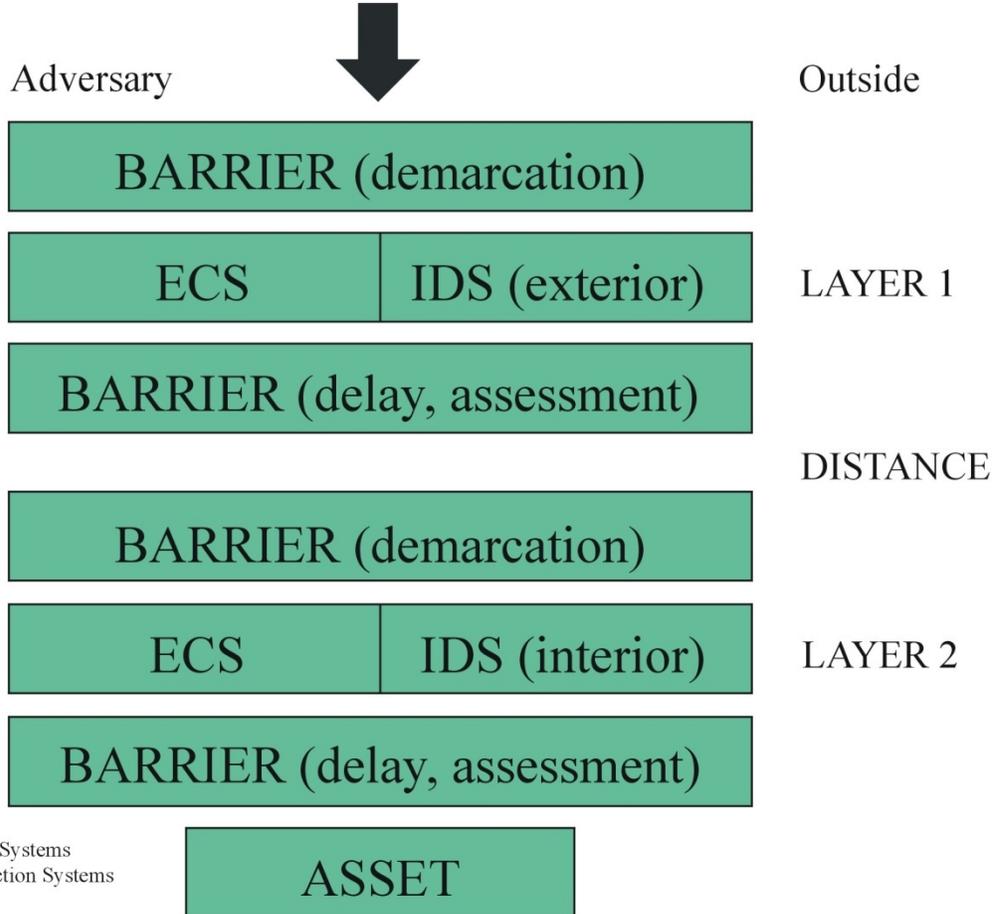
**PRIMER FOR THE ITIM Workshop  
January 2009**

**Integrated Physical Protection System**



# PRIMER FOR THE ITIM Workshop January 2009

## Schematic Adversary Path to an SNM Asset



**Note: Insiders have access to material areas by nature of their job functions and would not need to penetrate outer barriers.**

# PRIMER FOR THE ITIM Workshop

## January 2009

### **DEFINITIONS:**

#### **ASSESSMENT:**

The determination by a guard or an electronic system of the cause of an alarm and the extent of the threat.

#### **CENTRAL ALARM STATION:**

An installation which provides for the complete and continuous alarm monitoring, assessment and communications with guards, facility management and the response force.

#### **DEFENCE IN DEPTH:**

A concept used to design physical protection systems that requires an adversary to overcome or circumvent multiple obstacles, either similar or diverse, in order to achieve his objective.

#### **DESIGN BASIS THREAT:**

The attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated.

#### **GUARD:**

A person who is entrusted with responsibility for patrolling, monitoring, assessing, escorting individuals or transport, controlling access and/or providing initial response.

#### **INNER AREA:**

An area inside a protected area where Category I nuclear material is used and/or stored.

#### **INTRUSION DETECTION:**

Detection of an intruder by a guard or by a system comprising of a sensor(s), transmission medium and control panel to annunciate an alarm.

#### **PATROL:**

A function carried out by guards to inspect elements of physical protection at regular or irregular intervals.

#### **PHYSICAL BARRIER:**

A fence or wall or a similar impediment which provides penetration delay and complements access control.

#### **PROTECTED AREA:**

An area under surveillance, containing Category I or II nuclear material, and/or vital areas surrounded by a physical barrier.

#### **RESPONSE FORCES:**

Persons, on-site or off-site who are armed and appropriately equipped and trained to counter an attempted unauthorized removal of nuclear material or an act of sabotage.

#### **SABOTAGE:**

Any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the

## **PRIMER FOR THE ITIM Workshop**

### **January 2009**

health and safety of personnel, the public and the environment by exposure to radiation or release of radioactive substances.

#### **SECURITY SURVEY:**

A detailed examination, made by the State's competent authority, of proposed physical protection measures in order to evaluate them for approval.

#### **TRANSPORT:**

International or domestic carriage of nuclear material by any means of transportation beginning with the departure from a facility of the shipper and ending with the arrival at a facility of the receiver.

#### **TRANSPORT CONTROL CENTRE:**

An installation which provides for the continuous monitoring of vehicle location and security status and for communication with the transport vehicle, its guards, the response forces and the shipper/receiver.

#### **UNAUTHORIZED REMOVAL:**

The theft or other unlawful taking of nuclear material.

#### **VITAL AREA:**

An area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences.

# PRIMER FOR THE ITIM Workshop

## January 2009

### **Basic Material Control and Accounting (MC&A) Program**

#### **I. GENERAL INFORMATION**

##### **A. PURPOSE**

The MC&A program at a facility contain the MC&A elements of a graded safeguards program. While every MC&A program has as its objective the protection of nuclear materials (NM) assets, the program must also meet specific requirements defined by national and international agreements. A graded approach should be used to provide varying degrees of physical protection, materials accounting, and materials control to different types, quantities, physical forms, and chemical or isotopic compositions of nuclear material with the risks and consequences associated with the threat scenario. Specifically, the more attractive special nuclear materials (SNM) are to malevolent acts, the more stringent the controls are established.

##### **B. INTRODUCTION TO NUCLEAR ACCOUNTING AND CONTROL**

###### **Material Control**

Material control means the use of control and monitoring measures to prevent or detect loss when it occurs or soon afterward.

###### **Material Accounting**

Material accounting is defined as the use of statistical and accounting measures to maintain knowledge of the quantities of SNM present in each area of a facility. It includes the use of physical inventories and material balances to verify the presence of material or to detect the loss of material after it occurs, in particular, through theft by one or more insiders.

##### **C. OBJECTIVES OF MATERIAL ACCOUNTING AND CONTROL**

The primary objectives of the MC&A system are to demonstrate that materials are present, to provide timely detection of material loss, and to define the locations of loss, should they ever occur. This is achieved through a MC&A design the enables the facility to provide effective accounting and control for nuclear materials.

# PRIMER FOR THE ITIM Workshop

## January 2009

### D. BASIC CONCEPTS IN ACCOUNTING AND CONTROL

Accounting for the nuclear material inventory involves performing:

- Nuclear material measurements
- Tracking and verifying the location and quantities of nuclear materials
- Maintaining records and reports
- Performing data analysis to account for and detect loss of nuclear material
- Investigate and resolve apparent loss of nuclear material

### E. DEFINITIONS

Abrupt theft or diversion

A theft, or diversion, that is accomplished during a single occurrence.

Alarm Limit

A control limit established for an inventory difference which, when exceeded, requires immediate action and reporting. (Alarm limits are generally established at the 95 percent confidence level)

Credible Roll-up

A risk based evaluation of characteristics of the nuclear material and the security measures used to protect the material, based upon a performance standard. The determination of credibility of roll-up is unique to each facility. For example risk evaluation includes but is not limited to the following:

Material characteristics: quantity of material, chemical form, isotopic composition or purity, ease of separability, possibility of concealment, portability, radioactivity, self-protecting features

Security measures: containment strategy (types of drums or cans), accessibility, engineering controls, administrative controls, and protection strategies employed by the facility

Graded Safeguards

1. A system designed to provide varying degrees of physical protection, accountability, and material control to different types, quantities, physical forms, and chemical or isotopic compositions of nuclear materials consistent with the risks and consequences associated with threat scenarios

## **PRIMER FOR THE ITIM Workshop**

### **January 2009**

2. Providing the greatest relative amount of control and effort to the types and quantities of special nuclear material that can be most effectively used in a nuclear explosive device.

#### **Human Reliability Program (HRP)**

A Human Reliability Program (HRP), is designed to meet the objective of protecting the national security through a system of continuous evaluation of individuals working in positions affording unescorted access to certain materials, facilities, Information, and programs. The purpose of this continuous evaluation is to identify in a timely manner individuals whose judgment may be impaired by physical and/or emotional disorders, the use of illegal drugs or the abuse of legal drugs or other substances, the abuse of alcohol, or any other condition or circumstance that may represent a reliability, safety, and/or security concern.

#### **Key Measurement Points (KMP)**

Strategic locations at which measurements are made for loss detection analysis

#### **Limited Area (LA)**

A Security Area defined by physical barriers, used for the protection of classified matter and/or Category III quantities of special nuclear material, where protective personnel or other internal controls can prevent access by unauthorized persons to classified matter or special nuclear material.

#### **Material Balance Area (MBA)**

Is an area with physical boundaries in which:  
The quantity of nuclear material in transfers can be determined,  
A physical inventory can be determined, and  
A Material Balance can be established and evaluated for.

#### **Material Access Area (MAA)**

A Security Area defined by physical barriers and subject to access control, used for the protection of Category I quantities of special nuclear material or Category II quantities of special nuclear material with credible rollup to Category I quantity. A Material Access Area shall be contained within a Protected Area and shall have separately defined physical barriers constructed to provide sufficient delay time to control, impede, or deter unauthorized access. Area boundaries shall conform to the layered protection concept with a separate Material Access Area located within a separate and distinct Protected Area. Material Access Areas shall direct the flow of personnel and vehicles through designated portals.

#### **Protected Area (PA)**

## **PRIMER FOR THE ITIM Workshop**

### **January 2009**

A Security Area encompassed by physical barriers, surrounded by intrusion detection and assessment systems, and having access controls for the protection of Category II quantities of special nuclear material and/or to provide a concentric security zone surrounding a Material Access Area or Vital Area

Protracted theft or diversion

Theft or diversion that is accomplished by repeated occurrences.

Two person rule

As applied to the Materials Control Program, an access control and materials surveillance procedure that requires that at least two authorized people be present in locations with unsecured quantities of nuclear materials in Category I amounts or Category II amounts with roll up potential to Category I.

US Nuclear Material Categorization Category I

Vault or process area (e.g., glovebox line), MBA, MAA, and Protected Area

U235 HEU > 5000g

U233/Pu >2000g

US Nuclear Material Categorization Category II

Vault-type room or authorized process area, MBA, and Protected area

U235 HEU < 5000g and > 1000g

U233/Pu <2000g and >500g

US Nuclear Material Categorization Category III

Locked alarmed storage location or patrolled at intervals not to exceed 8 hours, MBA, and Limited security area

U235 HEU < 1000g and > 15g

U233/Pu < 500g and > 15g

US Nuclear Material Categorization Category IV

Locked storage location, Material balance area, and Limited security area and/or property protection

U235 HEU < 15g

U233/Pu < 15g

# PRIMER FOR THE ITIM Workshop

## January 2009

### SECTION 1 – MATERIALS ACCOUNTING

#### 1. ACCOUNTING SYSTEM

- a. The nuclear accounting system tracks the nuclear material inventories, accurately documents all transactions, and issues periodic reports. The system provides a complete audit trail on all accountable nuclear material from receipt through disposition.

#### 2. PHYSICAL INVENTORY PROGRAM

- a. The physical inventory program provides a performance test that validates the accuracy of the book values with a statistical result and may establish values to determine book closure. The book values may be updated on a continual basis, and the constant monitoring of other MC&A elements provides for accurate book values in a near real-time fashion. On some approved interval a shutdown and cleanout is performed in all processing areas to ensure all material is accounted for. The physical inventory is used to correct inventory records if an error is found.

#### 3. MEASUREMENT AND MEASUREMENT CONTROL PROGRAM

- a. The measurement and measurement control program ensures that all nuclear material (NM) measurement methods that support declared inventory values have a metrological basis. Inventory values should be traceable to recognized international standards. Programs should be place to assure that measurement systems used to determine values are in control prior to use. Measurements provide assurance that the NM values have been properly established and in conjunction with materials accounting provide a means to detect material that may have been lost, stolen, or diverted.

#### 4. MATERIAL TRANSFERS

- a. The accountability process for nuclear material transfers covers internal and external transfer activities. The MC&A objectives for material transfers are to deter and/or detect theft or diversion, by ensuring that all authorizations are in place, and provide an audit trail of transfers. In addition transfer checks and measurements and response to abnormal conditions ensure immediate detection.

#### 5. MATERIAL CONTROL INDICATORS PROGRAM

- a. Material Control Indicators program assesses key indicators to provide assurance that losses and unauthorized removals of nuclear material (NM) are detected in a timely fashion. Each indicator has an associated action limit. Some key indicators:
  - i. Administrative Inventory Adjustments reviews

## **PRIMER FOR THE ITIM Workshop January 2009**

- ii. Normal Operating losses reviews
- iii. Propagation of Variance reviews

### **6. SHIPPER/RECEIVER DIFFERENCE PROGRAM**

- a. A shipper/receiver difference evaluation is performed for all external transfers of accountable nuclear materials between the shipping facility and the receiving facilities. For those transfers covered by a

shipper/receiver agreement, the shipper/receiver difference is evaluated and resolved as described by the agreement. A shipper/receiver agreement will allow safeguards closure of the transaction and provide protocols for resolving any subsequent shipper/receiver difference resulting from later accountability measurements.

## **SECTION 2 – MATERIALS CONTROL**

### **1. ACCESS CONTROLS**

- a. The nuclear material (NM) access control program limits access to NM, NM data, MC&A system hardware, software, and other equipment and/or data to authorized individuals.
- b. Category I - Individuals must be Q-cleared and Human Reliability Program (HRP)-approved; they must be trained in safeguards procedures and security regulations and have a need to know and a need to access to the material. Security police officers control access to Category I MBAs. Visitors and other personnel must enter and exit by defined paths that have special nuclear material (SNM) detectors and metal detectors, either stationary or hand-held.
- c. Category II - If the MBA is credible for “roll-up”, all the access controls for Category I MBAs apply. If the MBA is not credible for rollup, all the access controls for Category I apply with one exception: personnel can have unescorted access when they meet all the following criteria:
  - i. personnel are either Q-or L-cleared,
  - ii. personnel know the MBA and the safeguards and security (S&S) regulations, and
  - iii. personnel have a need to know and a need to access.
- d. Category III – Access controls for Category III MBAs are similar to those for Category II MBAs. The difference is that Category III MBAs can use locked doors with key control or combination locks on the doors and administrative controls for the combinations. MBA personnel or the security police officer checks badge and maintains control logs for access.
- e. Category IV – Access controls for Category IV MBAs must have locked doors, requiring either keys or combinations. The MBA

## **PRIMER FOR THE ITIM Workshop**

### **January 2009**

custodian controls the distribution of keys and combinations administratively. A person with unescorted- access authorization must escort visitors. Personnel who have access to Category IV material must know the MBA and the S&S regulations and have a need to know and a need to access the material.

#### **2. MATERIAL SURVEILLANCE**

- a. Using a graded safeguards concept to establish a Materials Surveillance program (MSP) to detect unauthorized activities or anomalous conditions during normal operations and emergency conditions. The program is designed in combination with other safeguards elements to ensure that all reportable nuclear material is in authorized locations and the unauthorized material flows or transfers are detected in time to prevent unauthorized removal of material from the facility. The facilities implementation of the material surveillance program establishes MSPs to monitor and control NM, consistent with the material's quantity, attractiveness level, and accessibility.
  - i. Two-Person Rule – The safeguards two-person rule helps to ensure that no unauthorized activities occur in Category I or II MBAs.
  - ii. Daily Administrative Checks

#### **3. MATERIAL CONTAINMENT**

- a. The objective of the facility materials containment program is to ensure that nuclear materials controls are used in accordance with graded safeguards principles. Material containment measures are multilayered and provide defense-in-depth safeguards assurance against diversion, theft, or other compromises to the nuclear material inventory. In an effort to minimize the potential for unauthorized access to nuclear materials, the amount of material in use is limited to operational needs and by safety factors. Whenever practical it should be located in physical areas and administrative locations based on a graded safeguards approach.
- b. If an emergency or abnormal situation results in the evacuation of a Category I or II MBA, personnel not associated with the emergency recovery activities are not allowed to re-enter the Material Access Area until the following 3 conditions are met:
  - i. Evacuated personnel have been searched,
  - ii. The Material Access Area has been declared safe for re-entry, and
  - iii. A Daily Administrative Check has been performed if necessary.

#### **4. DAILY ADMINISTRATIVE CHECKS**

## **PRIMER FOR THE ITIM Workshop**

### **January 2009**

- a. The purpose of the Daily Administrative Check (DAC) program is to provide timely detection of obvious anomalies in Category I and II areas where roll-up to a Category I is credible.

#### **5. TAMPER INDICATING DEVICES PROGRAM**

- a. The TID-Indicating Device (TID) program provides a time-limited deterrent mechanism that will help detect any attempts to access the object being TID'd. Tampering is defined as the unauthorized opening of a container, package, door, or object to which a TID has been affixed or that is intrinsically sealed to provide the same type of deterrence as a TID. Intrinsically sealed items have physical characteristics that should their integrity be violated would immediately indicate tampering.
  - i. As part of the TID program individuals must complete training and continue to receive regular refresher training before they are authorized to apply, void, or remove TIDs. TIDs are a benefit only if they have been properly applied so that it is easy to detect when they have been compromised. TIDS are only considered a reliable safeguards element when they are used in conjunction with an effective material surveillance program.
  - ii. A TID program also includes a management element to track the disposition of all TIDs at a facility.

#### **6. SNM PORTAL MONITORING**

- a. THE SNM Portal Monitoring Program provides detection of SNM at the Material Access Area boundary and Protected Area access points. This detection assures that in combination with other detection elements (Metal Detector, X-Ray), undetected unauthorized removal of nuclear materials is not credible. All personnel and vehicles entering or leaving a Protected Area of Material Access Area are subjected to SNM monitoring. The ingress check is performed to create a baseline on the person, item, or vehicle, thus easing the assessment upon egress. Random metal shielding monitoring is performed at the Protected Area, while the Material Access Area is subject to 100% monitoring.

#### **7. WASTE MONITORING**

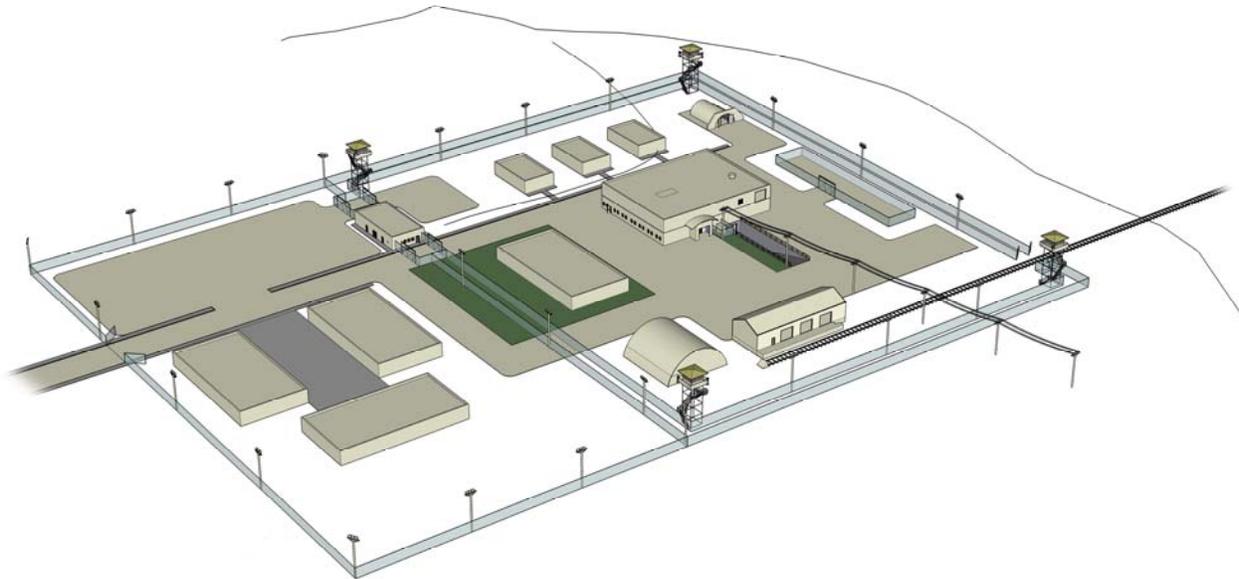
- a. The purpose of a facilities material control and accountability waste monitoring program is provide monitoring that will detect the theft or diversion of SNM by "piggy backing" on liquid, solid, and gaseous waste streams leaving a Material Access Area in time to prevent the removal of goal quantity. Waste monitoring equipment is

**PRIMER FOR THE ITIM Workshop**  
**January 2009**

maintained and controlled to ensure that the equipment is capable of detecting specified amounts of SNM. A response plan should be established for evaluating and resolving situations involving discharges exceeding facility specific limits if the situation is not satisfactorily resolved or if there is an indication of malevolent action.

# Hypothetical Facility Data Book

## The Uranium Research Facility (URF)



**November 9, 2007**  
**Final**

This page is intentionally blank.

## Table of Contents

|   |           |
|---|-----------|
| <b>Acronyms.....</b>  | <b>5</b>  |
| <b>1.0 Plant Overview.....</b>                                | <b>7</b>  |
| 1.1 General Description.....                                  | 7         |
| 1.2 Administrative Area .....                                 | 8         |
| 1.3 Protected Area .....                                      | 8         |
| 1.4 URF Processing Building .....                             | 11        |
| 1.5 Shipping and Receiving Building.....                      | 16        |
| 1.6 Finished Product Storage Bunker .....                     | 16        |
| 1.7 Support Buildings .....                                   | 16        |
| <b>2.0 Material on Site at the URF .....</b>                  | <b>17</b> |
| 2.1 Input Materials.....                                      | 17        |
| 2.2 Material Flows .....                                      | 17        |
| 2.3 Material Waste .....                                      | 18        |
| 2.4 Materials in Processing Building Vaults .....             | 18        |
| 2.5 Materials in Processing Area.....                         | 19        |
| 2.6 Materials Moved from the Processing Area .....            | 19        |
| 2.7 Materials in Basement Recovery Area.....                  | 20        |
| 2.8 X-ray Facility .....                                      | 20        |
| 2.9 Shipping and Receiving Warehouse .....                    | 20        |
| 2.10 Materials in the Finished Product Storage Bunker .....   | 20        |
| <b>3.0 Organization and Staffing.....</b>                     | <b>21</b> |
| <b>4.0 URF Material Control and Accounting System .....</b>   | <b>25</b> |
| 4.1 MC&A Organization.....                                    | 25        |
| 4.2 Material Balance Areas .....                              | 25        |
| 4.3 Measurements and Measurement Control Program .....        | 25        |
| 4.4 Physical Inventories .....                                | 26        |
| 4.8 Adjustments to Inventory.....                             | 27        |
| 4.9 Accounting Reports.....                                   | 27        |
| 4.10 Accounting System.....                                   | 27        |
| 4.11 Material Control.....                                    | 28        |
| 4.12 Personnel Access Control at Protected Area ECP.....      | 28        |
| 4.13 Lock and Key Control.....                                | 30        |
| 4.14 Badge and Visitor Control .....                          | 30        |
| <b>5.0 Operations at Gates and Portals at the URF .....</b>   | <b>32</b> |
| 5.1 Site Personnel and Vehicle Entrance (P2) .....            | 32        |
| 5.2 Protected Area Vehicle Gates (P5) .....                   | 32        |
| 5.3 Protected Area Personnel Access Control Point (P6) .....  | 32        |
| 5.4 Production Facility ECP (P8).....                         | 33        |
| <b>6.0 Physical Barriers and Alarms.....</b>                  | <b>34</b> |
| 6.1 Area Specific Access Controls and Physical Barriers ..... | 34        |
| 6.2 Likelihood of Detection for Sensors.....                  | 35        |
| 6.3 Barrier Penetration Times .....                           | 35        |
| 6.4 Miscellaneous Barriers .....                              | 35        |
| <b>7.0 Response Forces at the URF.....</b>                    | <b>36</b> |

**8.0 Other General Information..... 38**  
    8.1 Threat Data .....38  
**Appendix I..... 39**

**Figures**

Figure 1-1. URF Site Layout ..... 7  
Figure 1-2. Entry Control Building Layout ..... 10  
Figure 1-3. URF Processing Building Ground Level ..... 13  
Figure 1-4. URF Processing Building Basement Level..... 14  
Figure 1-5. URF Processing Building Mezzanine Level ..... 15  
Figure 2-1. Birdcage ..... 19  
Figure 3-1. URF Organizational Structure..... 21  
Figure 5-1. PA Entry Control Building..... 33

**Tables**

Table 1. Nominal URF SNM Inventory ..... **Error! Bookmark not defined.**  
Table 2. URF On-site Staffing Table ..... 22  
Table 3. Non-employee Access to URF Table ..... 24  
Table 4. Nominal URF SNM Inventory ..... **Error! Bookmark not defined.**  
Table 5. Access Controls and Physical Barriers ..... 34  
Table 6. Probabilities of Detection for Sensors ..... 35  
Table 7. Barrier Penetration Times ..... 35  
Table 8. URF Response Forces..... 36  
Table 9. Response Force Deployment Data..... 37  
Table 10. Average Response Force Times ..... 37

## **Acronyms**

|                 |  |
|-----------------|--|
| AA              | Administrative Area                        |
| BMS             | balanced magnetic switch                   |
| CAS             | Central Alarm Station                      |
| cm              | centimeter                                 |
| ECB             | Entry Control Building                     |
| ECP             | Entry Control Point                        |
| HEPA            | high efficiency particulate air            |
| HVAC            | heating, ventilation, and air conditioning |
| kg              | kilogram                                   |
| LEID            | limit of error of inventory difference     |
| m               | Meter                                      |
| MAA             | Material Access Area                       |
| MBA             | Material Balance Area                      |
| MC&A            | Material Control and Accounting            |
| NDA             | non-destructive analysis                   |
| PA              | Protected Area                             |
| PIR             | passive infrared                           |
| QA              | quality assurance                          |
| SNM             | special nuclear material                   |
| SRT             | Special Reaction Team                      |
| TID             | tamper indicating device                   |
| UO <sub>2</sub> | uranium dioxide                            |
| URF             | Uranium Research Facility                  |

This page is intentionally blank.

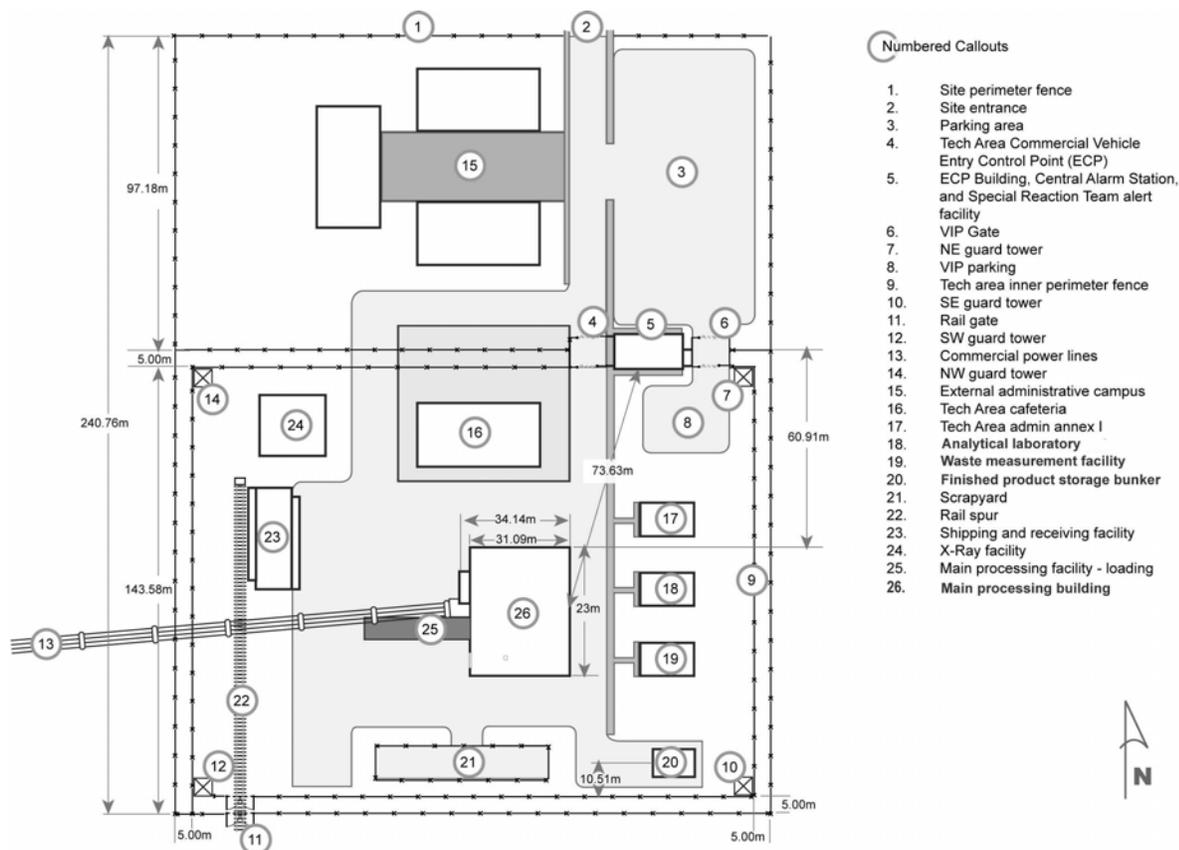
## 1.0 Plant Overview

### 1.1 General Description

The Uranium Research Facility (URF) is a national defense facility for the manufacture of uranium billets used in research. The site, which is located in a semi-arid high desert, is divided into two main areas: 1) a low security Administration Area, where much of the non-production activities take place (approximately 30% of the staff work in this area); and 2) a high security Protected Area (PA) which contains the main fabrication buildings, the production support buildings, storage vaults, road and rail transportation terminus, and the main cafeteria.

The main product of the URF is high-quality uranium billets that are used in nuclear material research. The input stream of this process begins with the delivery of uranium dioxide (UO<sub>2</sub>) powder. This powder is processed into raw ingots through a casting process. The raw ingots are then further processed into standard billets of specific size, shape, and weight. The waste from these processes goes into a uranium recovery stream that reintroduces the scrap material into the input stream. The finished product undergoes quality assurance (QA) checks and is then stored at a Finished Product Storage Bunker until it is transported by rail or truck to end users.

The simplified area diagram shown in Figure 1-1 illustrates both the major facilities of the URF and the defined material access areas.



**Figure 1-1. URF Site Layout**

## **1.2 Administrative Area**

The northern two-fifths of the URF Site is the Administrative Area (AA). This area is surrounded by a fence along three sides—known as the North Fence—and the PA fence along the southern side. The North Fence is 2.5 meters (m) high and is constructed of standard chain-link fabric fastened to metal poles. The site entrance gate (located on the north side of the site) is unlocked and open during normal working hours and is locked during off hours. During these off hours, personnel needing to enter the site must phone the guard in the Central Alarm Station (CAS) from a telephone at the gate. A guard is then dispatched to the gate to check the requester’s badge. Possession of a valid site badge is the only requirement for off-hour access.

The buildings in the AA are not alarmed and are unlocked except on weekends and holidays. Most senior management have keys to the outer doors of these buildings. Personnel have keys to their specific work areas. Personnel needing access to the buildings notify the guard, who opens the gate, escorts them to the building, and lets them in. When the personnel leave the building, they must inform the guard that they will no longer be in the building. The doors lock automatically behind the departing employee. The guard meets the employees at the gate to let them off-site. All keys are controlled by the guard force and are stamped “Do not duplicate.”

## **1.3 Protected Area**

There are nine buildings inside the PA perimeter. The main production building is the Process Facility located near the center of the area. There is also an Entry Control Building (ECB) that straddles the northern perimeter and houses pedestrian and vehicular entry control points, the CAS, and the Response Force Ready Room. Material shipments are processed through the shipping and receiving building. This building can support both road and rail transports. The Finished Product Storage Bunker, located in the southeast corner of the PA, is used to store finished products prior to shipping. A full service x-ray diagnostic facility, located in the northwest corner of the PA, is used for product quality control inspections. The PA also houses several small office buildings and the main cafeteria.

The analytical laboratory is situated between Technical Area Administrative Annex I and II. The first floor of the analytical laboratory is alarmed with a balanced magnetic switch (BMS) sensor on the door and passive infrared (PIR) sensors, providing interior volumetric intrusion detection. The windows also have iron bars across them. The guard force responds to any alarms that occur in this area. Members of the guard force have a master key that allows them to enter and investigate the analytical laboratory after an alarm occurs.

### **1.3.1 PA Perimeter**

The PA perimeter is comprised of two chain-link fences that are 2.5 m high and 5 m apart. Guard towers are located at each corner just inside of the PA perimeter. These guard towers, which are manned continuously, are high enough for the guards to see all the walls, the roof,

## **Exercise Data**

and entrances of the processing building. The towers have 360-degree viewing windows made of high-strength window glass.

The area outside the perimeter has a 20-m cleared zone that is bounded by trees in several locations. The terrain is relatively flat.

Patrols around the PA perimeter are conducted on the patrol road on a random basis. Patrols inside the PA perimeter are conducted by a guard on foot, also on a random basis. The lighting at the site is positioned as shown in the site specific data appendix.

### **1.3.2 Entry Control Building**

The ECB houses the PA's Personnel Entry Control Point (ECP), the CAS, and the Special Reaction Team (SRT) alert facilities. The CAS and SRT are in continuous operation. The ECP is open for normal entry during operational work hours, (7 am to 6 pm), but the outer doors are locked during off-hours. The east side of the ECB houses a quick response team of four persons, who respond to verified alarms in the area and provide key service to personnel needing access to normally locked areas. The northwest corner of the ECB houses the CAS, which is staffed by a senior guard.

The primary means for personnel and vehicle egress from the PA is through the ECB and its two vehicle portals. Vehicle entry through the PA perimeter is done through one of the gates. Most traffic is directed through the vehicle portal at the ECP (located on the northeast corner of the PA). The sliding gates are controlled from inside the ECP by one of the guards. Vehicle authorization is done by the guards with a visual recognition check.

Pedestrians enter the main door of the ECP and present their site badges to one of the guards sitting at the desk. If the guard approves the entry, the authorized person passes through the metal detector and on into the PA. The guard also randomly checks packages for contraband and investigates any metal detector alarms.

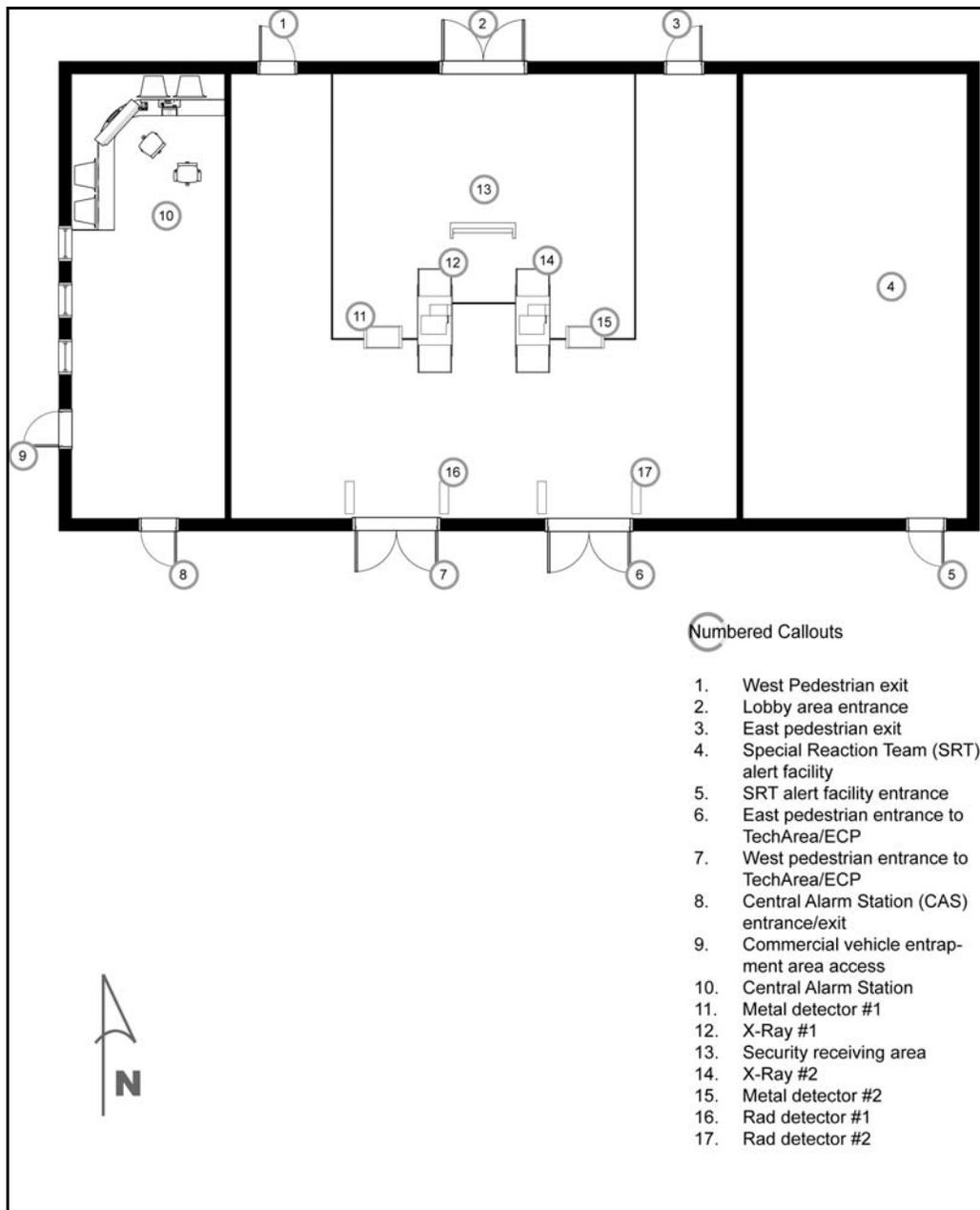


Figure 1-2. Entry Control Building Layout

## 1.4 URF Processing Building

All manufacturing processes are contained within the URF Processing Building. This building is a multi-story facility with a partial basement, ground, and mezzanine level. It has a total area of approximately 1700 square meters. The partial basement is the machine cooling fluid processing area, the ground floor is the processing area, and the mezzanine is the heating, ventilation, and air conditioning (HVAC) area. The production areas of the building are under negative pressure and all ventilation from these areas is passed through high efficiency particulate air (HEPA) and/or charcoal filters to minimize plant releases.

The URF Processing Building houses the following areas/operations:

- Casting Furnace Area—holds the two furnaces where UO<sub>2</sub> powder is cast into ingots.
- Billet Vault—finished ingots are stored here until needed by machining process.
- Special Nuclear Material (SNM) Machining Area—holds nine milling machines that can be configured to work as three lines of a three-step milling process or as nine individual stations. The milling process converts raw ingots into finished billets.
- Product Vault—stores finished billets before they are sent to QA or to the Finished Product Storage Bunker.
- QA Vault—In-process billet samples and final products are measured and tested in this vault. Only a limited amount of material may be in this vault at any one time.
- AA—general office area.
- Chip Vault—stores return stream waste from the Casting Furnace and Machining areas before it is reintroduced into the input stream.

### 1.4.1 Entryways in the Processing Building

The Processing Building (26 in Figure 1-1) is the primary material area. There is a main personnel entrance to the building and shipping entrances to both the nuclear material and non-nuclear material machine shop areas. The main personnel entrance allows access to the office areas, the non-nuclear material machining area, and the Process Area entry control portal. Pedestrians enter the main door and present their site badges to the receptionist at the desk. Emergency exits are located in both the administrative section and the processing areas. There are two chemical storage rooms that can only be accessed from outside and share the loading dock for the non-nuclear material machine shop. The Processing Building also has a shipping entrance to the partial basement that can be used for moving large equipment as well as an overhead shipping door to the mezzanine with a crane attachment for moving HVAC units into the mezzanine. There is grillwork over the duct ends on the mezzanine outer surfaces for the HVAC and filter system.

### 1.4.2 Processing Building—Construction Details

The emergency exit doors in the Processing Building are hollow-core metal industrial doors with panic hardware on the interior and a key lock on the exterior. The guards have the key to the lock for emergency response situations. The emergency exit doors are alarmed with BMS. The main entry doors are glass, equipped with BMS, and are set in a wall of windows. The foyer is used as a showcase to display information about the facility for visiting dignitaries. The exterior walls of the AA are made of 20-centimeter (cm) (8-inch) hollow concrete block. Each office has a window to the outside. The interior walls in the AA are

***Exercise Data***

typical sheetrock walls. There are no alarms in the offices or sensors on the office doors. The walls of the processing areas (the machining and casting areas) are constructed of 20-cm (8-inch) reinforced concrete. There are no windows to the outside in the processing areas. The roof in the processing areas is constructed of 14-cm (5.5-inch) reinforced concrete on metal decking.

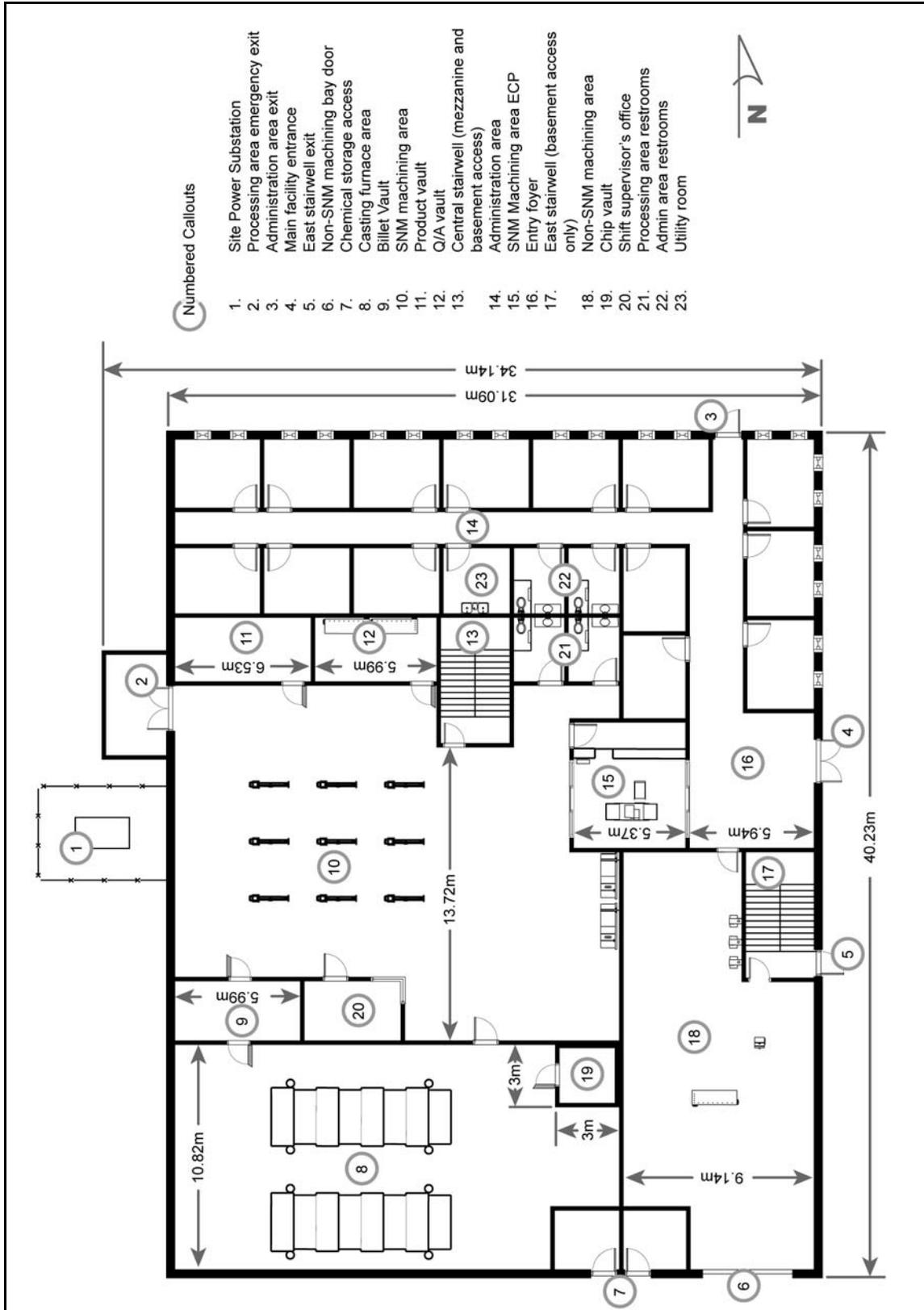


Figure 1-3. URF Processing Building (Processing Main floor)

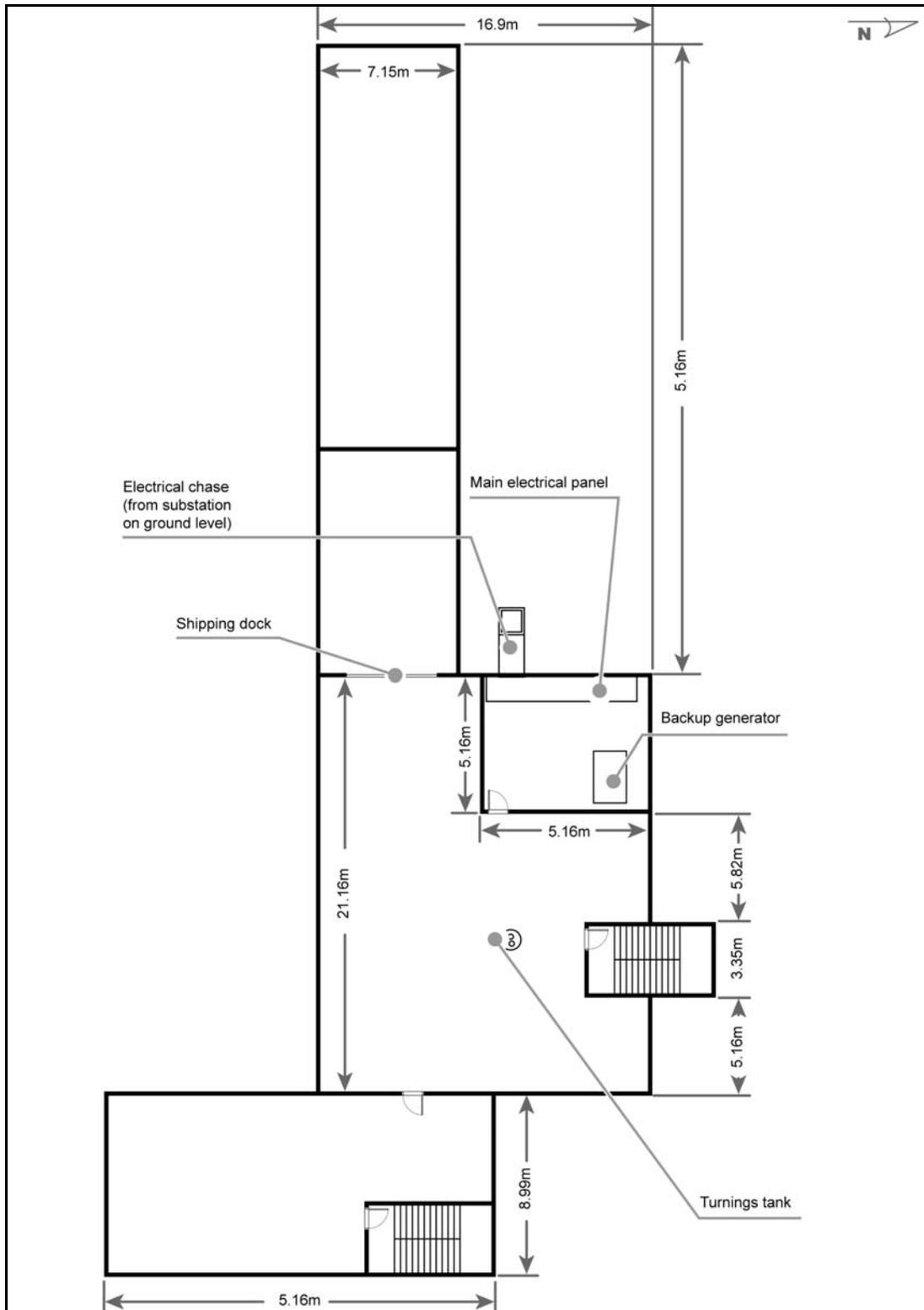


Figure 1-4. URF Processing Building (Basement)

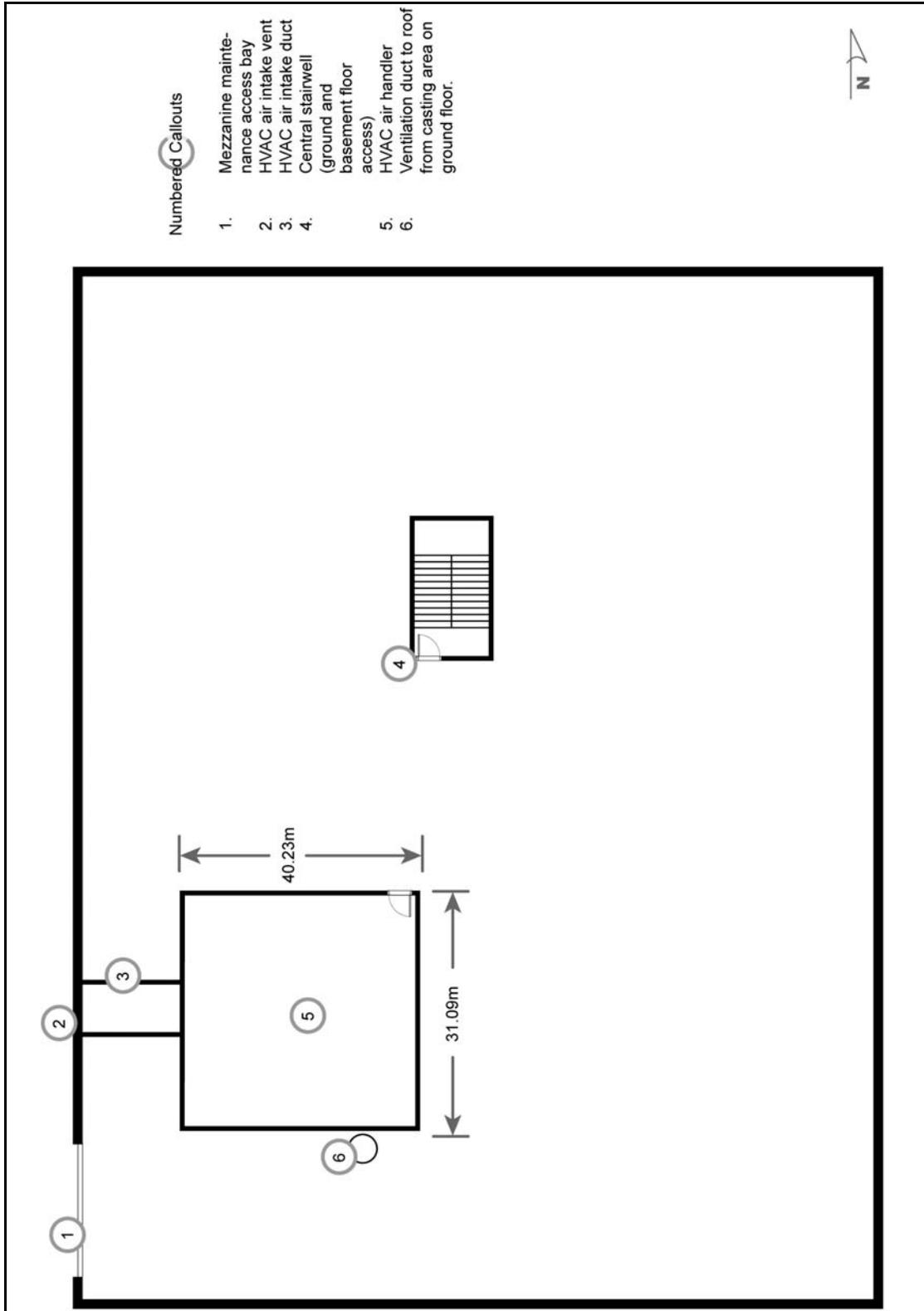


Figure 1-5. URF Processing Building (Mezzanine)

### **1.5 Shipping and Receiving Building**

The Shipping and Receiving building (23 in Figure 1-1) is a one-story building with loading docks on both sides (one for rail shipments and one for trucks). Although several cubical office spaces are inside, it is basically an open warehouse.

### **1.6 Finished Product Storage Bunker**

The Finished Product Storage Bunker (20 in Figure 1-1) is used to store nuclear material that was shipped in for recycling and finished products that are packed and ready to ship.

### **1.7 Support Buildings**

There are three single-story Support Buildings located east of the Processing Building: Administration (e.g., offices) (17 in Figure 1-1), the Analytical Laboratory (18 in Figure 1-1), and Waste Measurement Facility (19 in Figure 1-1). The Administration Building stores some classified material in safes. The Analytical Laboratory stores small quantities of nuclear material in the form of process samples and reference materials. The Waste Measurement Facility stores nuclear material in the form of waste drums.

## 2.0 Material on Site at the URF

**Table 1. Nominal URF SNM Inventory**

| Material Balance Area | Form of Material   | Allowable Material Inventory (wt % enrichment) |
|-----------------------|--|--|
| X-Ray Facility        | Uranium Metal – billets  | 5 kg U (>86.6%)                                |
| Product Bunker        | Uranium Metal – billets  | 300 kg U (>86.6%)                              |
|                       | UO <sub>2</sub> – loose powder   | 10 kg U (>86.6%)                               |
| Processing Building   | Uranium Metal – ingots   | 30 kg U (>86.6%)                               |
|                       | UO <sub>2</sub> – loose powder<br>Uranium Metal – scrap or input material (e.g., chips and turnings) | 50 kg U (>86.6%)                               |
|                       | Uranium Metal – billets  | 20 kg U (>86.6%)                               |
| Analytical Laboratory | Samples all forms  | 5 kg U (>86.6%)                                |

### 1.8 Input Materials

Input material consists of UO<sub>2</sub> powder or metal ingots formed at another plant and shipped in by request. Input material could also be un-irradiated billets that are to be recycled. Input material is stored in the product vault (11 in Figure 1-3) until needed for processing. Initially, the non-powder input material will be broken into “chips” and the chips will be transferred to the chip vault (19 in Figure 1-3) until needed for casting.

### 1.9 Material Flows

The annual throughput of the URF is approximately 1.7 metric tons or about 142 kg per month. This equates to the site being able to produce around 24 parts per month or 2 2/3 parts per lathe. Feed to the casting line is UO<sub>2</sub>, chips, turnings, flakes, etc. The feed for the casting line is stored in the chip vault (19 in Figure 1-3). When an ingot is needed for machining, and there is not one available meeting requirements in the billet vault (9 in Figure 1-3), a batch of chips and powder is put together that matches the requirements. This is done in the makeup area directly outside of the chip vault. A technician takes chips from various drawers in the vault or uses UO<sub>2</sub> powder to make up a batch. Samples for destructive assay and quality control are taken and sent to the Analytical Laboratory for analysis. The batch goes to casting and is matched with a form mold, assembled, and input to the casting line where material is heated, melted, poured into a mold, moved to a cooling chamber, cooled for 8 to 12 hours, taken from the mold, inspected for obvious flaws and/or problems, and put in the billet vault. If the ingot is flawed, it is also put in the billet vault and marked for breaking into chips again.

When manufacturing parts, the ingot or partially processed part is taken from the vault and moved to where it is needed in the SNM Machining Area (10 in Figure 1-3) (e.g., pressing, forming, lathes, punches, etc.). The ingots and partial parts are kept in small cages (birdcages) to enhance access control and to ensure criticality separation.

### **1.10 Material Waste**

Nuclear material in the form of waste is generated from various parts of the process. Waste is collected and placed in waste receptacles. On a regular schedule, the operation support personnel collect and package the waste into waste containers. Once packaged, this material is moved on a bi-weekly basis to the Waste Measurement Facility where it is assayed and the nuclear content determined. Once assay is completed, the waste packages are transferred to the shipping receiving facility to await transport for burial.

Clean waste is removed from the facility on a daily basis by operations support personnel on the 2<sup>nd</sup> shift. Waste is placed in dumpsters adjacent to the shipping dock. On a bi-weekly basis, a local garbage contractor has been contracted to pick up clean waste and transport it to a local dump site for disposal.

### **1.11 Materials in Processing Building Vaults**

The material stored in the Processing Building vaults is in various forms and quantities:

- UO<sub>2</sub> powder is stored in 0.5-kilogram (kg) cans.
- The chip vault has material in all sizes, shapes, and enrichments. When parts to be recycled come to the facility, they are crushed into small chips (typically between 200 and 500 grams each). These chips are classified by enrichment and stored in 2-liter stainless steel cans. The amount of material in each can may vary, but nuclear safety has established a limit of 1 kg of material in each can regardless of the enrichment. The cans are stored on open shelves in the vault.
- The billet vault contains 5-kg ingots. The ingots (after a cooling period) are collected and stored in plastic bags inside metal cans. These metal cans are an integral part of the birdcages (see Figure 2-1). The birdcages ensure correct separation distances and add some delay to the material. Each birdcage weighs 20 kg and is stored on the floor or on open shelves.
- The product vault contains the finished parts before they are shipped. These parts are stored in a special birdcage inside an inert gas package. The birdcage is essentially the same as the billet birdcage with a different container integrated into it. The finished products normally weigh between 2 and 3 kg (depending on the particular product being manufactured). The birdcage weighs 20 kg and is stored inside an expanded metal enclosure within the vault.

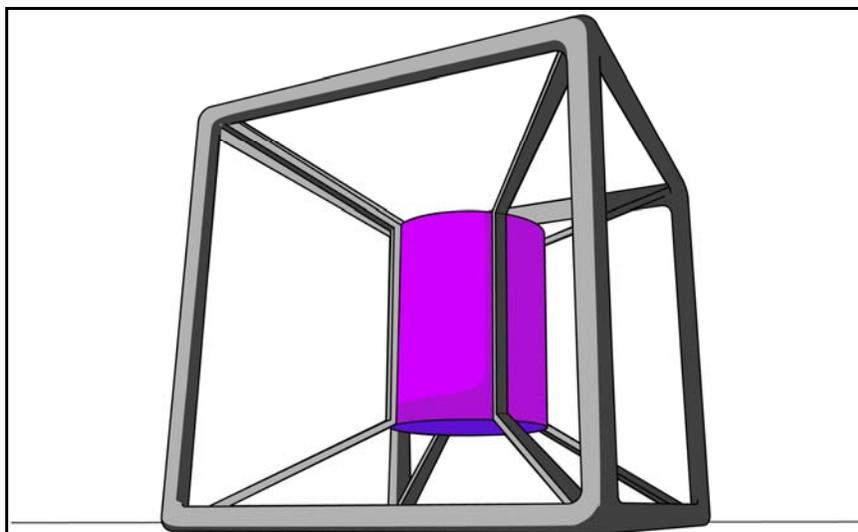


Figure 2-1. Birdcage

### 1.12 Materials in Processing Area

The amount of material exposed in the processing area at any one time in the material process can range from 6 to 50 kg, but is only present during the normal five-day work period. The birdcages with the material for specific machine input and output are moved by cart to the machine area at the start of each shift and are locked in place to a ring set in the floor. The material handlers have the key to lock the birdcage to the floor. The machinist has the key to open the cage to mount the material in the machine. Mounting the material can take 30 minutes, but dismounting can be done in 15 seconds. Since mounting takes so long on some machines, the material is left in the machine during breaks. When the machining is done, the product is put back in the birdcage and stored until it is collected on pickup rounds. The material custodian has a schedule of work and picks up the product soon after it is completed. If a problem occurs in the process that delays the product's scheduled pickup time, the machinist notifies his supervisor, who then notifies the Material Custodian. Material at various stages of machining is stored in the billet vault during non-working hours.

### 1.13 Materials Moved from the Processing Area

When a product is complete, it is moved to the quality control area for inspection. This area is set up as a vault since some materials may stay there for extended periods of time. Products will also be sent via inter-site convoy to the x-ray facility as part of quality control. Once material has passed quality control, it is packed in the material container and stored in the product vault. In preparation for off-site shipment, products are packaged in shipping containers and moved to the Finished Product Storage Bunker for storage. Material is shipped out on a schedule set by the military.

Other materials moved from the processing area include analytical samples and waste. Analytical samples are transferred from the Processing Area to the Analytical Laboratory on an as needed basis. Nuclear waste is removed bi-weekly when the facility is operating.

### **1.14 Materials in Basement Recovery Area**

Material is also accumulated in the recovery area in the basement. The turnings from the machines that are taken up in the cooling fluid are stored in the recovery area until a significant amount has accumulated. When weight differences indicate that greater than 2 kg of material is in the recovery area, recovery operations are undertaken and the fluid is filtered away from the material in a settling tank. When the fluid has been drawn away, the filter material is washed to recover the uranium. The recovered uranium is weighed, placed in a can, and sent back up to the chip vault for later re-use. A sample of the material is then taken and sent to the analytical lab to determine the isotope of the material (several different enrichments may be machined in one batch).

### **1.15 X-ray Facility**

During a normal test, parts are in the X-ray Facility for approximately six hours. When potential problems arise that need more investigation, parts can be left there overnight to preserve the diagnostic setup. When materials are in the X-ray Facility overnight, patrols place a seal on the door and check the seal every 30 minutes. The X-ray Facility is constructed like a vault—when material is left overnight, it requires 60 seconds for removal from the diagnostic test stand.

### **1.16 Shipping and Receiving Warehouse**

Shipments are put into the vault the same day they are received, but are often left in the shipping and receiving warehouse for two to three hours while the receiving paperwork is completed and weights and serial numbers are verified. While in the shipping and receiving warehouse, material is constantly attended and is checked by patrols every 30 minutes. Material in these locations are in 100-kg shipping containers.

A section of the warehouse is designated for storing nuclear waste containers. These containers are received from the Waste Measurement Facility after they have been assayed. Waste materials may be stored from several hours to several weeks until a truck load quantity is accumulated.

### **1.17 Materials in the Finished Product Storage Bunker**

The uranium in the Finished Product Storage Bunker consists of materials that were received for recycling or finished products that are packed and ready to ship. The material for recycling is on open shelves inside the Finished Product Storage Bunker. Received material is in approved shipping containers. The containers consist of a heavy gauge steel drum that has a lid secured by six bolts. After the bolts are tightened down to a specified bolt tension, each bolt has a tamper indicating device (TID) to indicate if any tampering has occurred. Inside the steel shipping container is the material container, which is secured by two packing sleeves. The material container is a heavy gauge steel container that also has a lid secured by six bolts. One of these bolts is sealed with a TID. The entire container weighs approximately 100 kg—the shipping container weighs 65 kg, the packing material weighs 7 kg, the material container weighs 25 kg, and the material weighs between 2 and 3 kg.

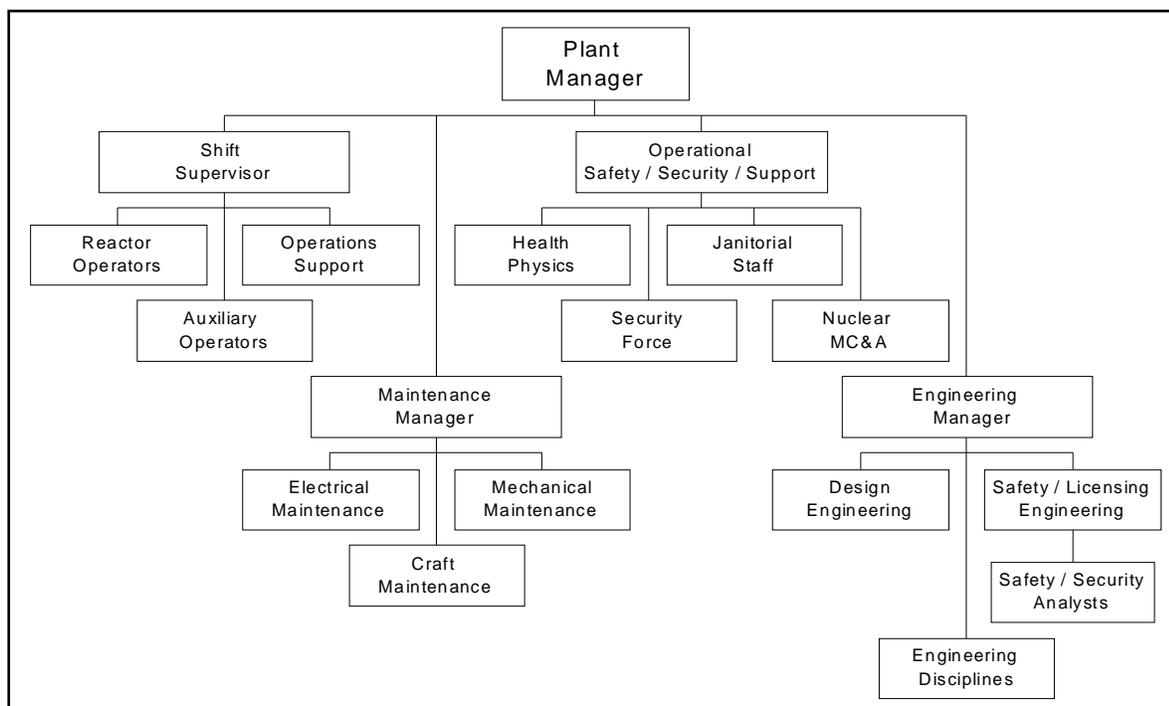
The product containers are inside an expanded metal locked enclosure and weigh 50 to 100 kg (depending on the type). The 100-kg product containers are essentially the same as the containers for received material. The 50-kg containers are designed to fit inside a larger shipping over-pack container and are not as robust as the 100-kg container. They are about

**Exercise Data**

one half as tall and the lids snap on with three quick-release levers. The same type of inner container is used for all items (with some variations in shape/size). Organization and Staffing

This section of the hypothetical facility description discusses the organization and staffing levels of the URF. It summarizes the access authorization of facility employees and other non-employees who have routine access to areas within the URF PA. During normal operation, 250 full-time employees work at the site in plant operations, maintenance, engineering, technical support, management, and administrative support positions. Of these, 182 employees require some access to the PA.

Figure 3-1 shows the overall organization of the URF. The following table shows the distribution of employees by job category, their routine plant access, and their levels of authority and knowledge about the plant.



**Figure 3-1. URF Organizational Structure**

**Table 1. URF On-site Staffing Table**

| <b>Position (Number)</b>   | <b>Routine Access</b>  | <b>Routine Authority/<br/>Responsibility</b>   | <b>Knowledge</b>   |
|--|--|--|--|
| Plant Manager (1)<br>(Plant Manager Org.)  | PA, All Inner Areas<br>(usually escorted)  | <ul style="list-style-type: none"> <li>• Overall direction</li> <li>• Not authorized to direct detailed facility operations</li> </ul>                             | General knowledge of plant operations, lacks detailed understanding of facility              |
| Shift Supervisor (three total with one per shift)<br>(Shift Supervisor Org.)                   | PA, All Inner Areas  | <ul style="list-style-type: none"> <li>• Detailed direction of all facility activities.</li> <li>• Direction obeyed without question in most situations</li> </ul> | Extensive, detailed knowledge about all aspects of facility design, layout, and operation    |
| Machining operator (6 total with nominal 4 per day shift)<br>(Operations Support Org.)         | PA, All Inner Areas  | <ul style="list-style-type: none"> <li>• Detailed direction of all machining activities</li> <li>• Under direction of shift supervisor</li> </ul>                  | Extensive, detailed knowledge about all activities in the machining area                     |
| Casting operator (6 total with nominal 4 per day shift)<br>(Operations Support Org.)           | PA, All Inner Areas  | <ul style="list-style-type: none"> <li>• Detailed direction of all casting activities</li> <li>• Under direction of shift supervisor</li> </ul>                    | Extensive, detailed knowledge about all activities in the casting area                       |
| Operations Support (6 total with nominal 4 per day shift)<br>(Operations Support Org.)         | PA, All Inner Areas  | <ul style="list-style-type: none"> <li>• Perform specific operations tasks under direction of machining and casting operators</li> </ul>                           | Specialized knowledge related to their duties, narrow knowledge of complete facility systems |
| Maintenance Manager (3 total with nominal 1 per shift)<br>(Maintenance Org.)                   | PA, All Inner Areas<br>(usually escorted)  | <ul style="list-style-type: none"> <li>• Overall direction to maintenance personnel</li> </ul>   | General knowledge of plant operations  |
| Electrical Maintenance (6 total with nominal 4 per day shift)<br>(Maintenance Org.)            | PA, All Inner Areas<br>as work orders specify                                      | <ul style="list-style-type: none"> <li>• Perform activities on specific systems pursuant to work orders and the plan of the day<sup>1</sup></li> </ul>             | Specialized knowledge related to their duties, narrow knowledge of complete facility systems |
| Mechanical Maintenance (6 total with nominal 4 per day shift)<br>(Mechanical Maintenance Org.) | PA, All Inner Areas<br>as work orders specify                                      | <ul style="list-style-type: none"> <li>• Perform activities on specific systems pursuant to work orders and the plan of the day</li> </ul>                         | Specialized knowledge related to their duties, narrow knowledge of complete facility systems |
| Administrative support (40, all day shift)<br>(Operational / Safety / Security Support Org.)   | Only to the outer office complex; occasional access to other areas requires escort | <ul style="list-style-type: none"> <li>• Administrative support</li> </ul>   | No working knowledge of facility systems   |
| Health Physics Technicians (4 total with nominal 3 per day shift)<br>(Health Physics Org.)     | PA, all Inner Areas and occasional escorted access to Storage Areas                | <ul style="list-style-type: none"> <li>• Monitor radiological conditions</li> <li>• Not permitted to work on plant equipment</li> </ul>                            | Specialized knowledge related to their duties, narrow knowledge of facility systems          |

<sup>1</sup> The plan of the day establishes the maintenance tasks to be performed each day and the systems to be removed from service for maintenance. The shift supervisor or his designee is required to be informed and provide authorization before a system is taken out of service for maintenance.

**Exercise Data**

| <b>Position (Number)</b>   | <b>Routine Access</b>  | <b>Routine Authority/<br/>Responsibility</b>   | <b>Knowledge</b>   |
|--|--|--|--|
| Guard Supervisor (5 total, 1 at all times)<br>(Security Force Org.)  | PA, all Inner Areas  | <ul style="list-style-type: none"> <li>• Direct activities of security force</li> </ul>  | No knowledge of facility systems, but knowledgeable about plant security systems and security procedures   |
| Alarm Station Operators (5 total, 1 at all times)<br>(Security Force Org.)                                     | PA, Central or Secondary Alarm station                                       | <ul style="list-style-type: none"> <li>• Monitor alarms and direct response under the direction of the Guard Supervisor</li> </ul>                                 | No knowledge of facility systems, but knowledgeable about plant security systems and security operational procedures                                 |
| Patrol Guards (10 total, 2 at all times)<br>(Security Force Org.)  | PA, all Vital Areas  | <ul style="list-style-type: none"> <li>• Routine patrol of PAs and non-radiological vital areas and respond to plant alarms</li> </ul>                             | No knowledge of facility systems, but knowledgeable about plant security systems and security operational procedures                                 |
| Post and tower Guards (34 total, 8 during the day shift, and 6 all other times)<br>(Security Force Org.)       | PA, all Vital Areas  | <ul style="list-style-type: none"> <li>• Staff access control and other security posts and respond to plant alarms</li> </ul>                                      | No knowledge of plant safety / operational systems or plant response to abnormal conditions, but knowledgeable about security operational procedures |
| Quick response force (20 total, 4 at all times)  |  |  | No knowledge of plant safety / operational systems or plant response to abnormal conditions, but knowledgeable about security operational procedures |
| Janitorial Staff (9 total, 5 during day shift and 2 at all other times)<br>(Janitorial Staff Org.)             | Outer office area, PA, and Specific Inner Areas dependent on work assignment | <ul style="list-style-type: none"> <li>• Cleaning and housekeeping</li> </ul>  | No knowledge of plant systems or security measures   |
| Material Balance Area Custodians (2 total, day shift)<br>(Nuclear Material Control and Accounting [MC&A] Org.) | PA, Inner Areas and Storage Areas  | <ul style="list-style-type: none"> <li>• Direct nuclear material inventories, authorize transfers</li> </ul>   | Knowledgeable about nuclear material status and inventory procedures, but no knowledge of facility systems   |
| Nuclear Material Technicians (2 total)<br>(Nuclear MC&A Org.)  | PA, Inner Areas and Storage Areas  | <ul style="list-style-type: none"> <li>• Perform nuclear material operations and inventories at the direction of Material Balance Area (MBA) custodians</li> </ul> | Knowledgeable about nuclear material status and inventory procedures, but no knowledge of facility systems   |

**Exercise Data**

| <b>Position (Number)</b>   | <b>Routine Access</b>  | <b>Routine Authority/ Responsibility</b>   | <b>Knowledge</b>  |
|--|--|--|---|
| Nuclear Material Accountability Technicians (2 total) (Nuclear MC&A Org.)  | Escorted access to PA, Inner Areas and Storage Areas                               | <ul style="list-style-type: none"> <li>Maintain paper accountability system and generate required nuclear material status, transfer, and inventory reports</li> </ul>                        | Knowledgeable about nuclear material status and inventory procedures, but no knowledge of facility systems                          |
| Engineering Support (3, all day shift) (Engineering Manager Org.)  | Only to the outer office complex; occasional access to other areas requires escort | <ul style="list-style-type: none"> <li>Support plant engineering activities</li> </ul>   | Specialized knowledge related to their duties   |
| Design, Mechanical, Electrical, Civil, Chemical and Nuclear Engineers (5, all day shift) (Design Engineering & Engineering Discipline Orgs.) | PA, Inner Areas with escort  | <ul style="list-style-type: none"> <li>Perform design activities and review performance and status of specific systems</li> </ul>  | Specialized knowledge related to design and performance of specific plant systems, moderate knowledge of complete facility systems  |
| Safety Engineers, (2 on day shift) (Safety / Licensing Engineering Org.)   | PA, Inner Areas with Escort  | <ul style="list-style-type: none"> <li>Analyze safety and impacts of proposed changes, develop / review procedures and procedure revisions, prepare documents for State regulator</li> </ul> | General knowledge of performance and roles of facility systems, but no detailed knowledge of operation of complete facility systems |
| Security Analysts (2)  | PA, Vital Areas with escorts   | <ul style="list-style-type: none"> <li>Perform security analysis activities and review performance and status of specific systems</li> </ul>   | Specialized knowledge related to design and performance of security systems   |

**Table 2. Non-employee Access to URF Table**

| <b>Type</b>                      | <b>Routine Access</b>  | <b>Routine Authority / Responsibility</b>   | <b>Knowledge</b>   |
|----------------------------------|--|---|--|
| Vendors                          | Only to the outer office complex; occasional access to other areas requires escort | <ul style="list-style-type: none"> <li>No authority over plant employees</li> </ul>   | No knowledge of plant systems, plant response to abnormal conditions, or security measures |
| State Safety/Security Inspectors | PA and Inner Areas; employee escort required for all access                        | <ul style="list-style-type: none"> <li>No direct authority over plant employees; however, suggestions are given great weight</li> </ul> | General knowledge of performance and roles of facility systems                             |

## 2.0 URF Material Control and Accounting System

This section of the hypothetical facility description discusses the URF procedures for nuclear material control and accounting (MC&A) and briefly describes the accounting system.

### 2.1 MC&A Organization

By letter of designation, the plant manager has delegated the responsibilities and authorities of all safeguard positions. A single individual is assigned the responsibility for technical coordination of the overall MC&A program. This position is referred to as the Material Control Manager. This position is separate from production and any other responsibilities that might give rise to a conflict of interest. In addition, there is a Measurement Control Coordinator, and, if needed, multiple Material Balance Area (MBA) Custodians assigned specific authorities, responsibilities, and locations reporting directly to the Material Control Manager.

### 2.2 Material Balance Areas

Four MBAs have been established at the URF. These are the Production Floor, the X-Ray Facility, the Analytical Laboratory, and the Finished Product Storage Bunker. All accountable SNM at the URF is maintained in one of these four MBAs. Non-accountable SNM in the form of waste can be present in the Waste Measurement Facility and the Shipping/Receiving Warehouse. The physical boundaries of the X-Ray Facility, Analytical Laboratory, and the Finished Product Storage Bunker MBAs are the structural boundaries of the respective building. The physical boundaries of the Production Floor MBA are the walls and access control point for the production area.

### 2.3 Measurements and Measurement Control Program

This program is under the control of the Measurement Control Coordinator. The measurement control program ensures the quality and reliability of the measurement data. This facility incorporates the following measurement control elements:

- various mass weighing stations
- destructive laboratory analysis and sampling
- non-destructive analysis (NDA) measurement systems
- weekly calibration or operability checks with reference standards
- a sampling program to ensure that portions of the bulk material taken for measurement are representative of the bulk material
- control programs associated with all measurement systems to ensure the quality of data generated

The Measurement Control Coordinator maintains the equipment and standards in a locked room in the non-nuclear material portion of the Processing Facility and is responsible for the proper use and calibration of the equipment.

In addition, the MC&A organization controls and issues TIDs for use throughout the facility. MBA Custodians are the only personnel trained to apply and remove TIDs.

## 2.4 Physical Inventories

A physical inventory is conducted every two months under normal conditions. The physical inventory consists of a 100% inventory of items or containers with TIDs and measurement of a statistical sample of items. The measurements are NDA measurements and the attributes are compared to the book data. Discrepancies are tracked in the measurement control system. If a measurement is beyond the control limits for that measurement from the recorded value, the item in question is subjected to additional confirmatory measurements, including opening the container and, if required, conducting destructive measurements.

Data obtained during the physical inventory, data from measurements during the material reconciliation period, and control program data are used to calculate the Limit of Error of Inventory Difference (LEID). Special inventories are conducted when custodial responsibilities are changed, items are believed to be missing, inventory differences exceed established control limits, and other abnormal occurrences take place. These special inventories may be limited to a single vault or MBA, depending on the occurrence. However, the facility may be impacted depending on the circumstances. Investigation of inventory differences between accounting records and physical inventory results will be performed to determine the cause.

**Table 4. Nominal URF SNM Inventory**

| Material Balance Area | Form of Material   | Allowable Material Inventory (wt % enrichment) |
|-----------------------|--|--|
| X-Ray Facility        | Uranium Metal – billets  | 5 kg U (>86.6%)                                |
| Product Bunker        | Uranium Metal – billets  | 300 kg U (>86.6%)                              |
|                       | UO <sub>2</sub> – loose powder                                     | 10 kg U (>86.6%)                               |
| Processing Building   | Uranium Metal – ingots   | 30 kg U (>86.6%)                               |
|                       | UO <sub>2</sub> – loose powder                                     | 50 kg U (>86.6%)                               |
|                       | Uranium Metal – scrap or input material (e.g., chips and turnings) |  |
|                       | Uranium Metal – billets  | 20 kg U (>86.6%)                               |
| Analytical Laboratory | Samples all forms  | 5 kg U (>86.6%)                                |

## 2.5 Measurement Points

Material measurements may take place at several points in an item’s existence in the processing area. Material is normally measured on the following occasions:

- A receipt measurement is taken within five days of receipt.
- Depending on whether the mass limit exceeds 2 kgs, an item may require a measurement for internal transfers between MBAs.
- Measurements are taken when modifications are made to materials in the machining or casting process.
- Measurements are taken as part of item monitoring along the process path.

## **Exercise Data**

- Final product measurements are taken before containerization and TID application.
- A final measurement is performed within five days before shipment.
- Waste is measured at the Waste Measurement Facility as packages are generated and staged.

## **2.6 Shipping and Receiving**

Items received are booked on shipper's values for element and isotope content. When shipments are received, the item count and item identifiers are verified against the shipping documents. Items shipped are sent based upon the book values for the element and isotope content. Where shipper receiver differences are identified on shipped items, the shipper-receiver difference is resolved by adjusting the URF book values to the receiver's measured values, as long as the difference does not reflect a difference in the number and identity of the items shipped and received.

## **2.7 Item Monitoring**

In addition to the fixed periodic physical inventories, the process area has further designated several Inventory Control Locations, which provide the capability to physically locate (or confirm the location of) items in a timely manner. This capability to localize losses (or thefts) of SNM allows for the identification of the mechanism for any such loss (or theft) in a more time-sensitive manner. Process boundaries are selected primarily on the basis of manufacturing control; however, this division also enables managerial assignment of specific material handling and control responsibilities, if required.

## **2.8 Adjustments to Inventory**

Adjustments are made to inventory on the basis of the measurements at the key measurement points. Accountability values for billets or ingots are based on DA or weight. Inventory is adjusted for the difference between the measured input versus the final accountability weight. Adjustments are also made based on waste that is removed from the process as established by NDA in the Waste Measurement Facility.

## **2.9 Accounting Reports**

URF submits material balance reports for each MBA within 30 days of completion of a physical inventory. Nuclear material transaction reports for the MBA covering all transactions during the inventory period are submitted with the material balance report. URF provides a telephone report to the State Regulator within four (4) hours of determining that an item cannot be accounted for. This report is followed up with a written report within 24 hours of this determination.

## **2.10 Accounting System**

URF employs a computer-based accounting system that is managed and operated by personnel who are not authorized access to SNM. The computer on which the accounting system is operated is a standalone machine. Entry of or access to accounting data or modification of the accounting software requires authorization via a password system. All data is input to the URF computer accounting system from paper records (e.g., inventory sheets and material transfer forms), which are uniquely numbered, accounted for, signed by

the individuals completing them, and retained for the life of the plant. The URF accounting software is commercially procured and is not modified by plant staff.

## **2.11 Material Control**

Physical control of the material is established through several individual programs. Access controls limit personnel access to the processing area and additional access controls further limit personnel access to the processing floor in the processing building. Once on the processing floor, procedural measures limit access to material to those with an established need for access. The MBA Custodians for the various process area locations authorize all material movements. Material access is further enforced through the use of the two-person rule. Any time a material location is accessed, two persons must be present. Two persons must also be present when material is on the machines on the process floor. The machine operator is one of the two persons and the machining supervisor or MC&A Representative acts as the second person for all material being worked on at any given time. Access to specific parts is controlled through the use of locks on the birdcages containing materials. The machine operator is only issued the keys for the work that is at his station for the day.

Transfers of samples to the Analytical Laboratory and waste to the Waste Measurement Facility are handled by Operations Support Personnel. Since these are Category III/IV quantities, the two person rule is not applied.

## **2.12 Personnel Access Control at Protected Area ECP**

### **2.12.1 Entry Process**

Personnel entering the PA must process through the ECP. The ECP is open from 0700 to 1800 Monday through Friday. Authorized personnel enter the area through the middle double doors to the ECP and process through contraband portal detectors. All hand-carried items are placed in plastic boxes and processed through the X-ray machine. Personnel then proceed through the portal metal detector. If they trigger an alarm, they may walk back through the portal, search themselves to determine what caused the alarm, place that material on the X-ray belt, and walk through the portal again. If they do not trigger another alarm, they may collect their materials and enter into the processing area. If they set off the portal alarm a second time, they must be searched by the guards with a hand-held unit. The guards also monitor the X-ray video for contraband. There are two guards at the portal area to process personnel.

### **2.12.2 Exit Process**

Personnel exiting the PA enter the ECP through the double doors and pass through the nuclear material monitoring portal. If they do not set off the alarm, they continue through the exit doors (east and west). If there is an alarm, the guards will stop the person passing through the alarming portal and call the Health Physics personnel, who will respond to determine the cause of the alarm. If the portals alarm when personnel are passing through them to enter the area, the person is stopped and questioned regarding possible reasons the alarm might have sounded and Health Physics is called to check the equipment. That exit door will be locked until the monitor is certified to be in working order.

The ECP for the processing floor in the processing building is similar to the area ECP and contains the same equipment (although the metal detection threshold is lower).

### 2.12.3 Contraband Detection Equipment

All contraband detection equipment and alarm equipment at the ECPs is maintained and tested by the technical unit of the guard force. The X-ray and metal detection equipment is function-tested every shift. The guard supervisor walks through the metal detection portal (with his sidearm) to ensure that it alarms and will run a test item (such as a step wedge) through the X-ray detector to check the operability of the X-ray system. Since access to a test source requires the coordination of the Health Physics or MC&A staff, the nuclear material portals are only tested via the self-test button (which only tests the light and tone alarms).

The contraband detection equipment is performance-tested on a monthly basis. A special test item kit is used to test the metal detection portal. This kit contains sealed weapons that bound the less detectable, commercially available handguns. Two technicians from the technical unit perform the test; one passes the units through the field at specific locations, and the other reads through the test procedure and records results. The sensitivity of the X-ray unit is tested with a test kit containing various synthetic explosive materials, various gauges of wire, and various shielding materials. If any equipment is found to fall below specified performance specifications, it is readjusted per the manufacturer's instructions and tested again. The nuclear material portal monitor is also checked at this time. The Health Physics personnel bring a radiological source (Americium) and take it through the portal in several configurations (near the top of the portal, near the middle, and near the bottom). The Health Physics personnel make any required adjustments to the equipment since the technical unit of the guard force does not receive training in nuclear detection equipment. However, someone from the technical unit must be present while the Health Physics personnel make these adjustments.

The nuclear material portal monitor controls and sensitivity adjustment are contained in a locked panel on one side of the portal. The head of the Health Physics Department locks the key in a safe in his office. The unit is wired to the security power system for the CAS which has an uninterruptible power supply (UPS) and a generator backup. The alarm for the unit is local with a light and tone alert. The metal detector sensitivity adjustment and controls are located in the top panel of the unit. There is a key pad for user input and a code is used to access the setup and adjustment menus. If the supervisor code is entered, several basic sensitivity programs that come with the unit from the factory can be selected with one key stroke. These units are also wired into the CAS power system. The alarm for these units is local and consists of an alarm tone and a light bar indication of alarm strength. Due to overrunning the capacity of the CAS power system, the X-ray units are powered by normal facility power. Sensitivity adjustment control is through software with a password required for access to any operation other than normal screening. A trained operator must watch the screen to notice if contraband is passing through the system. There is no automatic alarm indication.

If a system malfunction is noted in the daily report, it is required to be worked on within 24 hours. During normal operating hours, there are always two technicians available to ensure adequate oversight of repair work. On weekends, a guard watches over the work since there is usually only one technician available. After any maintenance or repair work, the system is tested by the technician and then is put back into service.

#### **2.12.4 Intrusion Detection Systems**

The technical unit of the guard force is also responsible for testing intrusion detection systems in place at the site. The critical intrusion detection systems are tested monthly (e.g., in the vaults) and other systems are tested quarterly on a rotational basis. All tests are carried out according to a schedule that the guard force commander approves annually. BMS testing is considered to be completed by normal opening of doors for routine activities and is not specifically tested in the scheduled tests. The testing performed on a regular basis is classified as performance testing and is done to determine how the sensors detect people approaching a target. The technicians perform the walk test on interior sensors by starting at a logical starting point (e.g., a door or window) and progressing toward the target until an alarm is signaled. This is repeated at least ten times and at least once from all possible entry locations. Any missed detections are reported. If the problem is from the equipment or furniture in the detection area, the occupants will be contacted and will work with the technical unit to resolve the issue. If the blocking items cannot be moved, more detectors may be installed.

Two members of the technical unit conduct the tests—one reads through the procedure and record results while the other performs the walk test. Two members of the technical unit will also be on hand for any repairs to ensure oversight of repair work. Once repairs are made, the system will be performance-tested by the technical unit and turned over to the CAS.

All intrusion detection systems have an installed battery backup power system and are connected to a stand-by generator. A fully charged battery powers the intrusion system for at least ten minutes which is sufficient time for the generator to be switched on. Backup batteries are checked when the systems are performance-tested. Generators are tested every three months on weekends by facilities management personnel.

All intrusion alarm communications wiring is run in conduit and has DC line supervision. All junction boxes are either sealed or have tamper switches. The data-gathering panels are locked with a special key that only the technical unit has access to. They are also protected with tamper switches.

#### **2.13 Lock and Key Control**

The technical unit is also charged with installing locks, making keys, and changing combinations. One master locksmith and several clerks assist with key control. The office for the lock unit is in Administrative Annex 1. All combinations and key blanks are stored in a safe. Records of keys and work requests and completions are kept on a computer in the office. Only the master locksmith and the clerical staff have the password to the system. Keys for office doors, building doors, and padlocks are cut on a special key blank registered to the site. There are not supposed to be any master keys. Once a certain number of keys have been lost (greater than 5%), all locks are re-cored with a new keyway. All combination locks have the combinations changed at least annually. However, the combination is changed immediately if there is a change in personnel.

#### **2.14 Badge and Visitor Control**

The site uses a new badge printing process that prints directly on plastic badge stock. The entire system has changed to this new type of badge. A background has been designed and a tamper-resistant overlay has been provided for all national sites to use. Although each site

### ***Exercise Data***

has a special alpha-numeric identifier that shows where the particular badge was issued, the badges are designed to allow access at all affiliated sites. The badge office (in the Administrative Building outside of the PA) prints all employee and visitor badges for this site. Badge stock is locked in a safe in the badge office when it is not occupied. Different colors around the border of the badge signify different access authorizations. A legend of these designators is posted in entry control points to quickly resolve any questions regarding access.

### **3.0 Operations at Gates and Portals at the URF**

#### **3.1 Site Personnel and Vehicle Entrance (P2)**

Personnel are permitted access through an access control point after verification that they have a current site badge. The guard controlling access is required to verify that the picture matches the badge holder and that the badge has not expired or been revoked. There is an access control office in the Administration Building that issues permanent and temporary badges for access to the plant. Exiting personnel are not checked.

Vehicles authorized routine entry to the site are provided with decals. The security officer(s) on duty permit vehicles to enter upon verifying the vehicle decal and the badges of all vehicle occupants. Temporary vehicle passes may be obtained at the Administration Building with appropriate authorization from site management.

When a delivery vehicle arrives, the guards review the manifest and shipping documents to verify that the truck has a delivery for the institute. The guards then contact the recipient of the delivery to verify that it is expected. Once this is done, the guards inspect the truck for contraband. If the delivery vehicle passes inspection, it is permitted entry to the site. Exiting vehicles are not checked.

#### **3.2 Protected Area Vehicle Gates (P5)**

These gates are normally closed and locked with high-security padlocks. When a vehicle arrives, an ECP guard verifies that the driver either has a URF badge permitting access to the URF PA, or has the required escorts. Once the guard has verified that the vehicle is expected, the guard inspects it for contraband. If the vehicle passes inspection, the guards contact the CAS to request that the PA intrusion detection system zone at the gates be placed in the access mode. The guards then unlock the vehicle gates to permit the vehicle entry to the URF PA. After the vehicle has entered the PA, the gates are locked and the PA intrusion detection system zone at the gates is returned to the secure mode.

Upon exit, vehicles are scanned with a radiation monitor to ensure that there is no contamination and are searched for SNM. Once guards verify that the vehicles are not contaminated and do not have unauthorized SNM, the vehicles are permitted to exit. The contamination scan and SNM search are performed inside the PA with the vehicle gates locked.

#### **3.3 Protected Area Personnel Access Control Point (P6)**

Personnel entering the PA undergo a search for contraband by passing through metal and explosive detectors. Hand-carried items are X-rayed and passed through metal detectors. Suspicious items are physically searched. Individuals who fail the metal detector search are either searched again with a hand-held metal detector or are subjected to a pat-down search. The personnel then enter the URF PA via a key-card-accessed door. The guards who perform the badge checks have a “panic” button that will override the key card reader, freezing the doors and precluding any entry to the PA. In a site emergency, the doors can also be reconfigured to permit egress from the PA to facilitate evacuation. The layout of the entry control section of the URF PA entry control point is shown in Figure 5.1.

Personnel exiting the PA undergo a search for SNM by passing through metal and SNM detectors. Hand-carried items are X-rayed. Suspicious items are physically searched.

## Exercise Data

Individuals who fail the metal detector search are either searched again with hand-held metal detectors and SNM detectors or are subjected to a pat-down search. After verification that individuals are not carrying SNM, they undergo a badge exchange—turning in their URF picture badges and key cards and picking up their Site picture badges. The personnel then exit the URF PA via unlocked doors.

### 3.4 Production Facility ECP (P8)

The URF Production Area includes the controlled areas within the Production Building where a Category I quantity of SNM is accessible. The key card system for entry to and exit from this area requires two key cards in order to open the door.

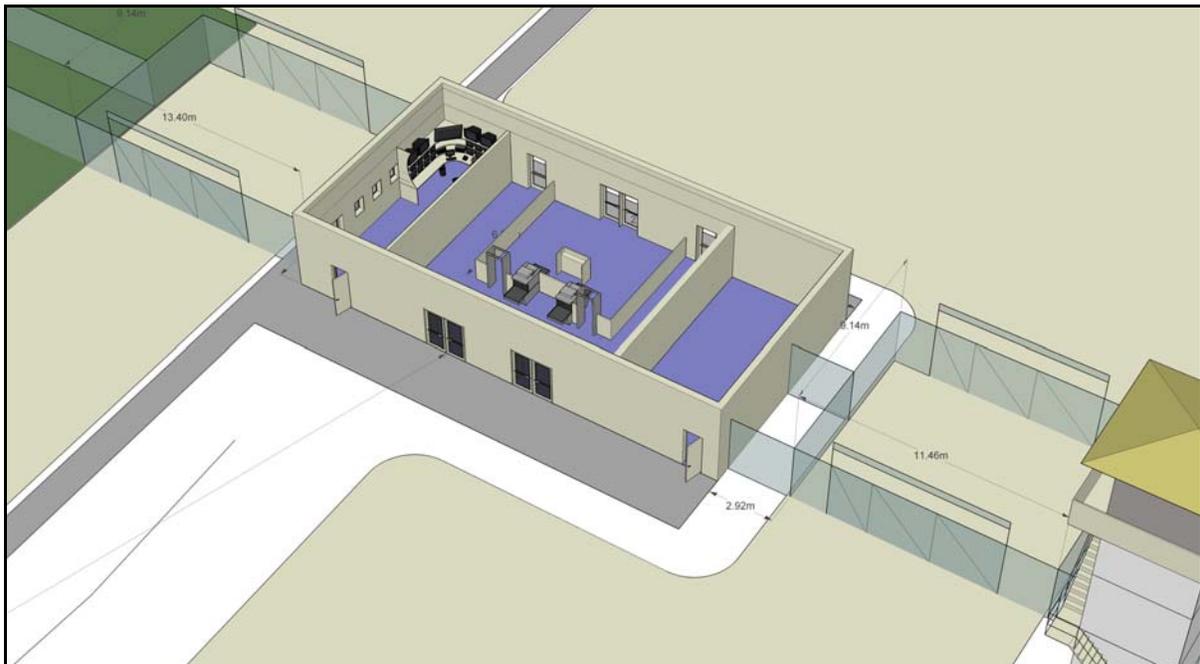


Figure 5-1. PA Entry Control Building

## 4.0 Physical Barriers and Alarms

The URF Site is surrounded by an unalarmed 2.5-meter-high chain-link fence to delineate the legal boundary and keep out trespassers. The URF PA is surrounded by two 2.5-meter-high chain-link fences with an alarmed isolation zone between the two fences. The vital areas within the URF are enclosed by 20-cm-thick reinforced concrete walls with access through 0.75-cm steel-plate water tight doors. Access is controlled by an electronic key card system that releases a door latch. In addition, each door is alarmed with a BMS to detect unauthorized entry.

### 4.1 Area Specific Access Controls and Physical Barriers

**Table 3. Access Controls and Physical Barriers**

| Controlled Area                 | Access Controls   | Physical Barriers                                   | Detection Devices                        |
|---------------------------------|---|---|--|
| AA                              | Employee badge  | Chain-link fence; vehicle gate                      | Guard checks                             |
| PA                              | ECP   | Perimeter Intrusion Detection and Assessment System | Perimeter sensors; tower guards          |
| ECP                             | Employee badge with guard present to ensure correct procedures at metal detectors and SNM detectors | Security doors; walls                               | Guard; metal detectors and SNM detectors |
| X-Ray Facility                  | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| Finished Product Storage Bunker | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| Production Building             | Entry control portal  | Security doors; walls; guard                        | Metal and SNM detectors                  |
| Product Vault                   | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| QA Vault                        | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| Chip Vault                      | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| Casting Furnace Area            | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |

## 4.2 Likelihood of Detection for Sensors

The following qualitative likelihoods of detection should be used in all sub-group exercises.

**Table 4. Probabilities of Detection for Sensors**

|                          | No Equipment | Hand Tools | Power Tools | High Explosives | Land Vehicle |
|--------------------------|--------------|------------|-------------|-----------------|--------------|
| <b>Exterior Sensors</b>  |              |            |             |                 |              |
| Generic                  | M            | M          | M           | M               | H            |
| Multiple complementary   | H            | H          | H           | H               | N/A          |
| <b>Interior Sensors</b>  |              |            |             |                 |              |
| Generic                  | M            | M          | M           | M               | N/A          |
| Multiple complementary   | H            | H          | H           | H               | N/A          |
| <b>Position Sensors</b>  |              |            |             |                 |              |
| Position Switch          | M            | L          | L           | L               | N/A          |
| Balanced Magnetic Switch | H            | H          | H           | H               | N/A          |
| <b>People</b>            |              |            |             |                 |              |
| General Observation      | VL           | VL         | L           | H               | H            |
| Directed Observation     | M            | H          | H           | H               | H            |

## 4.3 Barrier Penetration Times

The following barrier penetration times should be used in all sub-group exercises. All times are in seconds.

**Table 5. Barrier Penetration Times**

| Barrier Description                 | No Equipment | Hand Tools | Power Tools | Explosives |         | Land Vehicle |
|-------------------------------------|--------------|------------|-------------|------------|---------|--------------|
|                                     |              |            |             | Stage 1    | Stage 2 |              |
| Wood studs and sheetrock            | 60           | 30         | 30          | 30         | 0       | N/A          |
| <b>Doors</b>                        |              |            |             |            |         |              |
| 30-cm wood door with metal sheeting | Infinite     | Infinite   | 530         | 160        | 30      | N/A          |
| 5-cm wood door                      | Infinite     | 12         | 12          | 12         | 0       | N/A          |
| 0.75-cm steel plate door            | Infinite     | 300        | 30          | 30         | 0       | N/A          |
| Class V or VI vault door            | Infinite     | 480        | 60          | 60         | 0       | N/A          |
| <b>4.4 Miscellaneous Barriers</b>   |              |            |             |            |         |              |
| Steel turnstile                     | Infinite     | 72         | 18          | 18         | 0       | N/A          |
| High-security padlock               | Infinite     | 90         | 60          | 30         | 0       | N/A          |
| Tempered glass window               | 5            | 5          | 5           | 5          | 5       | N/A          |

## 5.0 Response Forces at the URF

Table 6. URF Response Forces

|   |   |
|---|---|
| <b>Types of Response Force Personnel</b>  | The response force consists of two types of onsite security personnel: <ul style="list-style-type: none"> <li>• Unarmed guards</li> <li>• Armed guards, including tactical response teams</li> </ul>  |
| <b>Responsibilities of Response Force</b> | These security personnel are responsible for: <ul style="list-style-type: none"> <li>• assessment of alarms</li> <li>• administrative duties, such as access control and key service</li> <li>• routine patrol and staffing of fixed posts</li> <li>• response to all security alarms</li> </ul> <p>All posts and patrols have defined policies and procedures with which the guard force must comply.</p>  |
| <b>Supervisors</b>                        | For each shift, one supervisor is present to supervise the guards that conduct administrative duties, patrols, and intrusion alarm response.  |
| <b>Equipment: Unarmed Guards</b>          | All <b>unarmed guards</b> are equipped with: <ul style="list-style-type: none"> <li>• a straight baton</li> <li>• one set of handcuffs</li> <li>• a small flashlight</li> <li>• a handheld radio</li> </ul>   |
| <b>Equipment: Armed Guards</b>            | All <b>armed guards</b> are equipped with: <ul style="list-style-type: none"> <li>• an automatic pistol with a fully loaded magazine</li> <li>• two spare magazines of ammunition</li> <li>• a straight baton</li> <li>• one set of handcuffs</li> <li>• a small flashlight</li> <li>• a handheld radio</li> </ul>  |
| <b>Equipment: Tactical Response Team</b>  | The tactical response team members are equipped with: <ul style="list-style-type: none"> <li>• an automatic pistol with a fully loaded magazine</li> <li>• an automatic assault rifle with a fully loaded magazine</li> <li>• two spare magazines of ammunition for each weapon</li> <li>• a straight baton</li> <li>• handcuffs</li> <li>• flashlight</li> <li>• handheld radio</li> <li>• body armor is readily available in the response force vehicles</li> </ul>   |
| <b>Alarm Stations and Communication</b>   | The <b>Central Alarm Station (CAS)</b> is located in P-1 and is staffed by a minimum of one guard at all times. This guard is responsible for the assessment of alarms and communication to the response force. The security force supervisor is routinely at the CAS.<br>The CAS is equipped with: <ul style="list-style-type: none"> <li>• 100-watt radios that can communicate to all posts and patrols within the boundaries of the Institute</li> <li>• 2 telephone lines—one is linked to each fixed post via a buried telephone cable and the second is a direct link to the offsite response force located in the city</li> </ul> <p>All hand-held radios and fixed posts are equipped with a duress switch to allow sending the CAS a covert signal of unauthorized activity. When the CAS receives a duress alarm, the response force is contacted.</p> |

|                                  |  |
|----------------------------------|--|
| <b>Security Force Deployment</b> | The response force is deployed as described in Table 9 below. The security posts and site layout are illustrated in the area diagrams. |
|----------------------------------|--|

**Table 7. Response Force Deployment Data**

| Post No.      | Description                         | No. of Guards |           |
|---------------|-------------------------------------|---------------|-----------|
|               |                                     | Day Shift     | Off-Shift |
| P-1           | CAS (unarmed)                       | 1             | 1         |
| P-2           | Site Personnel and Vehicle Entrance | 1             | 0         |
| P-3           | PA Vehicle Gate                     | 1             | 0         |
| P-4           | PA Personnel Portal                 | 2             | 1         |
| P-5           | Production Facility ECP             | 2             | 1         |
| P-6           | Roving Patrol inside URF (unarmed)  | 2             | 2         |
| P-7           | Tactical Response                   | 4             | 4         |
| <b>Totals</b> |                                     | <b>13</b>     | <b>9</b>  |

|                         |   |
|-------------------------|---|
| <b>Response Process</b> | All alarms are received at the CAS. For alarms that cannot be assessed via closed-circuit television, the CAS operator dispatches the nearest available guard to assess the alarm. If the assessment indicates a situation that cannot be handled by a single unarmed guard, the CAS operator dispatches additional guards. |
|-------------------------|---|

**Table 8. Average Response Force Times**

| Alarm Location                  | Response Time <sup>2</sup> |
|---------------------------------|----------------------------|
| PA Fence                        | 30 seconds – 2 minutes     |
| X-Ray Facility                  | 30 seconds – 2 minutes     |
| Finished Product Storage Bunker | 30 seconds – 3 minutes     |
| Production Floor                | 30 seconds – 2 minutes     |

<sup>2</sup> The variation in response times reflects the varying locations from which guards may be dispatched to respond to the alarm.

## 6.0 Other General Information

### 6.1 Threat Data

- Items were recently confiscated from a political terrorist group's hiding place, which was located less than 200 kilometers from the URF. The items included internal engineering drawings of the URF with circles drawn around the Finished Product Storage Bunker; various weapons, including automatic weapons; some explosives; and evidence of correspondence and communication with a foreign terrorist group. Interviews with property owners and residents indicated the group consisted of three to five men.
- Intercepted communications from a neighboring country indicates that a large terrorist group has tried to acquire a large quantity of nuclear material.
- The local police report that several Special Forces members were offered large cash payments to provide special training to unidentified individuals.
- A major bank robbery was committed in the capital two months ago. Four robbers escaped with a large amount of money. Investigation shows the bank vault was breached by the sophisticated use of high explosives stolen from the local army base.
- Nationally, many thefts of highly valuable items have occurred. The crimes do not appear to be related to each other. It is speculated that several groups committed the crimes. Organized crime may be involved.
- A recent meeting of the Atomic Energy Ministry included a special session on analysis of threat to nuclear facilities and material. No substantiated data on threat were available. However, the general feeling among members was that a threat to nuclear facilities does exist.
- During a meeting of the Industrialists Society, concern was expressed by managers of corporations that some of their employees had been approached by unnamed groups to help them carry out theft of valuable equipment and materials from the corporations. The employees had been offered large amounts of money.
- An analysis of the backgrounds of the employees of URF and of the population of the community did not provide any information that would suggest a concern of threat to the URF.
- There have been some internal disputes over labor issues at the URF in the past five years.
- Local news media publicized the recently upgraded security system at the URF as the latest in modern security system design with full International Atomic Energy Agency compliance.
- Two institute employees were recently caught stealing equipment and were terminated from the facility.
- A new employee drug and competency-screening program was recently introduced.
- A site-wide inventory recently discovered that several controlled site drawings were missing.
- Local reports of upcoming layoffs at the plant have recently been announced in the local news.
- The general attitude of the community is tolerant of the URF. However, certain activist groups have protested the plant during religious holidays.

## Upgrades Toolbox

|   |
|---|
| <b>Physical Protection</b>  |
| Provide vehicle search mirrors  |
| Provide hand-held SNM and metal detectors for searches, and explosive detection equipment                                   |
| <b>Material Control</b>   |
| Establish training on basic material control principles   |
| Review, enhance, and implement material control procedures  |
| Post static guards while NM is accessed or transferred  |
| Establish procedure for two-person rule   |
| Secure NM in safes or repositories<br>(includes the purchase of new safes and repositories if necessary)                    |
| Ensure visual administrative checks of NM<br>(frequency could vary depending upon level of PP)                              |
| Implement electronic key control dispensers and procedures  |
| Provide adhesive type tamper-indicating seals   |
| Establish control fence<br>(used to delineate a control zone; the fence has no detection capabilities)                      |
| Monitor NM waste leaving protected areas<br>(using hand-held SNM and metal detectors)                                       |
| Conduct random searches for personnel exiting protected areas<br>(using hand-held SNM and metal detectors)                  |
| Implement CCTV for personnel surveillance   |
| Provide loop type tamper-indicating seals   |
| Provide photo id badge manufacturing capability   |
| Install pedestrian and vehicle portal monitoring (metal & SNM) and hardened guard posts                                     |
| Provide advanced technology TIDs  |
| Employ advanced automated access control w/ smart card technology DP required   |
| <b>Material Accounting</b>  |
| Provide training on basic accounting principles   |
| Establish MBAs  |
| Appoint a custodian for each MBA  |
| Review, enhance, and implement reporting procedures   |
| Consolidate materials to reduce number of items   |
| Containerize material<br>(to convert to items and to reduce the number of items)  |
| Conduct internal audits of accounting system  |
| Review, enhance, and implement transfer procedures  |
| Record all off-site receipts and shipments  |
| Transfer checks for material crossing MBAs<br>(refer to text for actions included in a transfer check)                      |
| Implement a paper accounting system<br>(typically <500 items and/or < 30 moves/mo.)   |
| Perform RBI   |
| Review, enhance, and implement inventory procedures<br>(including reconciliation of inventory differences)                  |
| Conduct a semi-annual physical inventory of Cat I and II items in storage<br>(frequency could vary depending upon level PP) |

## Upgrades Toolbox

---

|   |
|---|
| Conduct visual administrative check of nuclear material<br>(frequency could vary depending upon level PP)   |
| Calculate hold-up using site history  |
| Conduct verification measurements of materials received from off-site<br>(Category IC and II material within 30 calendar days)  |
| Perform verification measurements of materials received from off-site<br>(Category III material within 120 calendar days, or on input to process)   |
| Perform confirmation measurements of materials received from off-site<br>(Category I and II material within 10 working days of receipt)   |
| Take verification measurements of bulk materials entering an MBA<br>(Category I and II material within one day of receipt)  |
| Take confirmation measurements of any materials entering an MBA<br>(Category I and II material within one day of receipt)   |
| Conduct bi-monthly physical inventory of Cat I and II items in-process  |
| Implement bar-coding systems  |
| Implement a simple computer accounting system<br>(typically 500-1000 items and/or 30-1000 moves/mo.)  |
| Provide electronic scales and balances  |
| Perform physical inventory using measured values<br>(especially after an abnormal event, such as suspected theft)   |
| Perform statistical analysis of measured materials  |
| Provide accountability measurement equipment using DA<br>(Davies-Gray titration)  |
| Provide accountability measurement equipment using non-destructive analysis<br>(neutron coincidence counters, active well coincidence counters, gamma spectrometers, alpha spectrometers, etc.) |
| Provide advanced computer accounting system<br>(typically >1000 items and/or > 1000 moves/mo.)  |
| Implement fiber optic computer networks (DP required)   |
| Provide standards and references  |
| Provide mass spectrometry<br>(DP required)  |
| Provide calorimetry<br>(DP required)  |
| Perform hold-up measurements  |
| Perform waste measurements to close material balance<br>(cleaning pipes, filters, etc.)   |
| Report MC&A data to national system (FIS)   |
| Perform confirmation measurements of materials received from off-site<br>(Category IA materials –ASAP or within one day of receipt)   |
| Perform confirmation measurements of materials received from off-site<br>(Category IB materials – within five working days of receipt)  |
| Perform verification measurements of materials received from off-site<br>(Category IB materials – within 10 working calendar days)  |
| Conduct weekly count of Category 1A items   |
| Perform monthly physical inventory of Category 1A items   |
| <b>General</b>  |
| Conduct training on procedure development   |

---

**Appendix I****Upgrades Toolbox**

---

|   |
|---|
| Conduct training on comprehensive PP and MPC&A upgrades and principles      |
| Provide training on MPC&A system operations, maintenance and sustainability |
| Provide training program management   |
| Implement test to determine the performance of MPC&A upgrades               |
| Conduct exercises to determine the performance of staff                     |
| Validate the performance of procedures                                      |
| Verify the accuracy of equipments, measurements, and controls.              |



# Lecture 1

---

## Course Overview – Insider Introduction



Lawrence Livermore  
National Laboratory



# Learning Objective

---

- **Become familiar with the overall course, its structure, content and goals**
- **Understand the insider analysis approach**
- **Be introduced to instructors and students**

# Insider Protection Course Description

---

**A systematic analysis approach that is used to evaluate the ability of MPC&A administrative and technical measures to meet performance requirements based on the capabilities and attributes of a defined insider threat**

# Scope of Training Course

---

- **This Insider Protection Course is designed to apply to nuclear and radiological:**
  - **Facilities**
  - **Materials**
- **This course is designed to provide a structured analysis approach that can be used to prevent or detect two types of malevolent events**
  - **Theft and/or diversion of nuclear materials**

# Insider Course Structure

---

- **The course consists of 8 days of training, including:**
  - **Lectures**
  - **Discussion – large and small groups**
  - **Group Exercises**
  - **Case Studies**
  - **Demonstrations**



# Course Modules and Schedule

---

## Module

- 1 Course Overview
- 2 Personnel Measures
- 3 Administrative Measures
- 4 Technical Measures
- 5 Quantifying Material Control-Physical Protection  
Material Accounting
- 6 Detection and Assessment
- 7 Hypothetical Facility
- 8 Target Characterization
- 9 Insider Characterization
- 10 Case Studies

# Course Modules and Schedule

---

## **Module**

- 11 Insider Analysis Methodology
- 12 Abrupt Theft Analysis
- 13 Protracted Theft Analysis
- 14 Upgrade Analysis
- 15 Maintaining System Effectiveness
- 16 Advances in Insider Technologies
- 17 Closing Discussion

# Course Goals

---

- **By applying a structured analysis approach, participants will be able to:**
  - **Understand US best practices**
  - **Identify and characterize potential Insider threat groups**
  - **Identify potential targets of interest to Insider adversaries**
  - **Identify and characterize MPC&A measures to protect against the Insider**
  - **Estimate the likelihood of an Insider causing undesirable consequences**
  - **Evaluate the effectiveness of current and planned MPC&A systems against an Insider threat**
  - **Identify and evaluate MPC&A upgrades that could reduce the risk of Insider malevolence**
  - **New understanding of MC&A and complexities of protracted theft**

# Role of Design Basis Threat and Risk Based Designs

---

*DOE Policy mandates the following steps:*

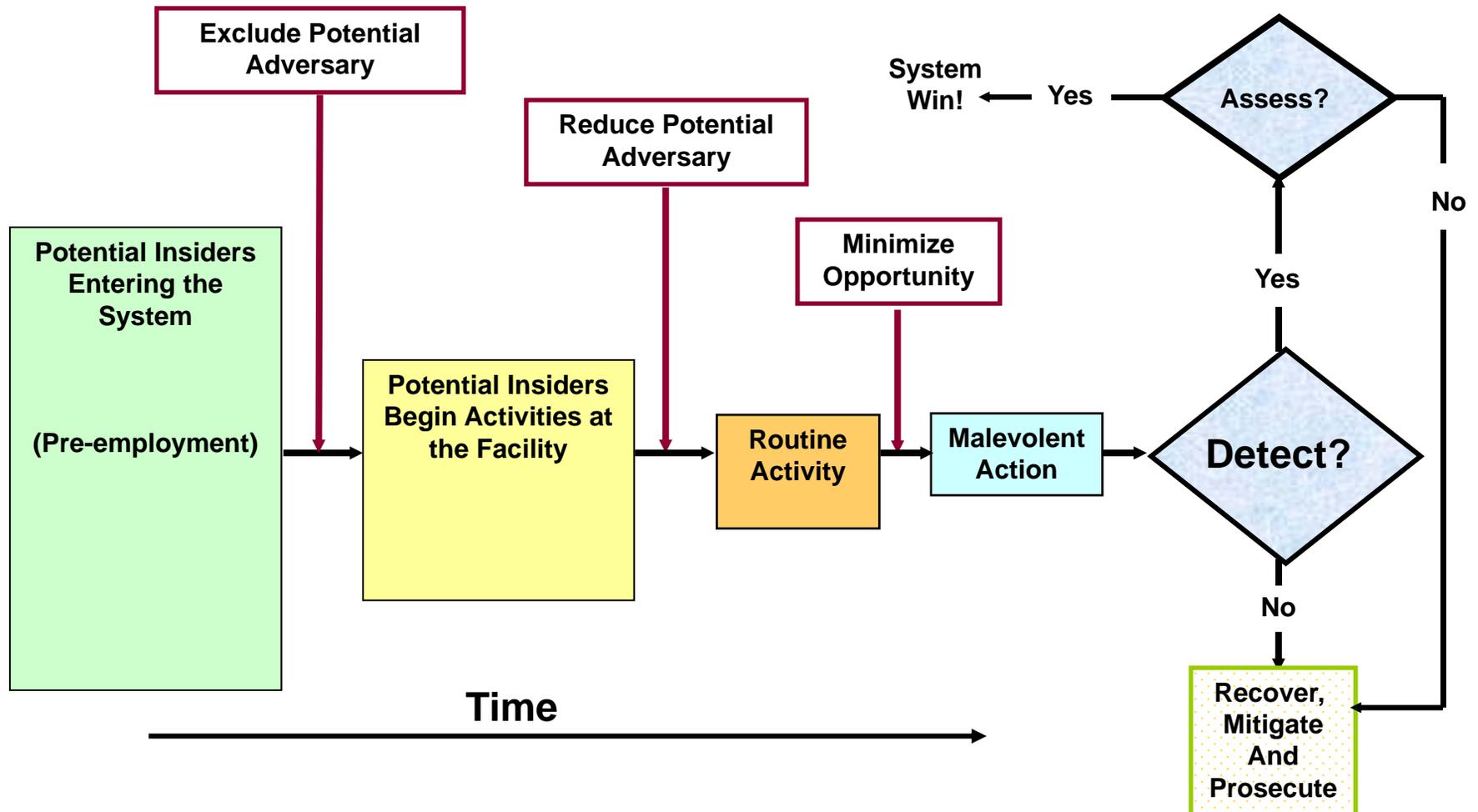
- Define the Scope of Work
  - Operating manufacturing or power production processes that store, handle, or process nuclear materials suitable for proliferation.
- Analyze the Risk (e.g., DBT)
  - Establish the risk or threat for the scope of work being undertaken. (e.g., Insider or outsider theft or sabotage)
- Develop and Implement MPC&A Measures
  - Note: rest of the course will be devoted to the MPC&A measures and their evaluation with respect to how they mitigate and control the identified risks.

# Insider Analysis Approach

---

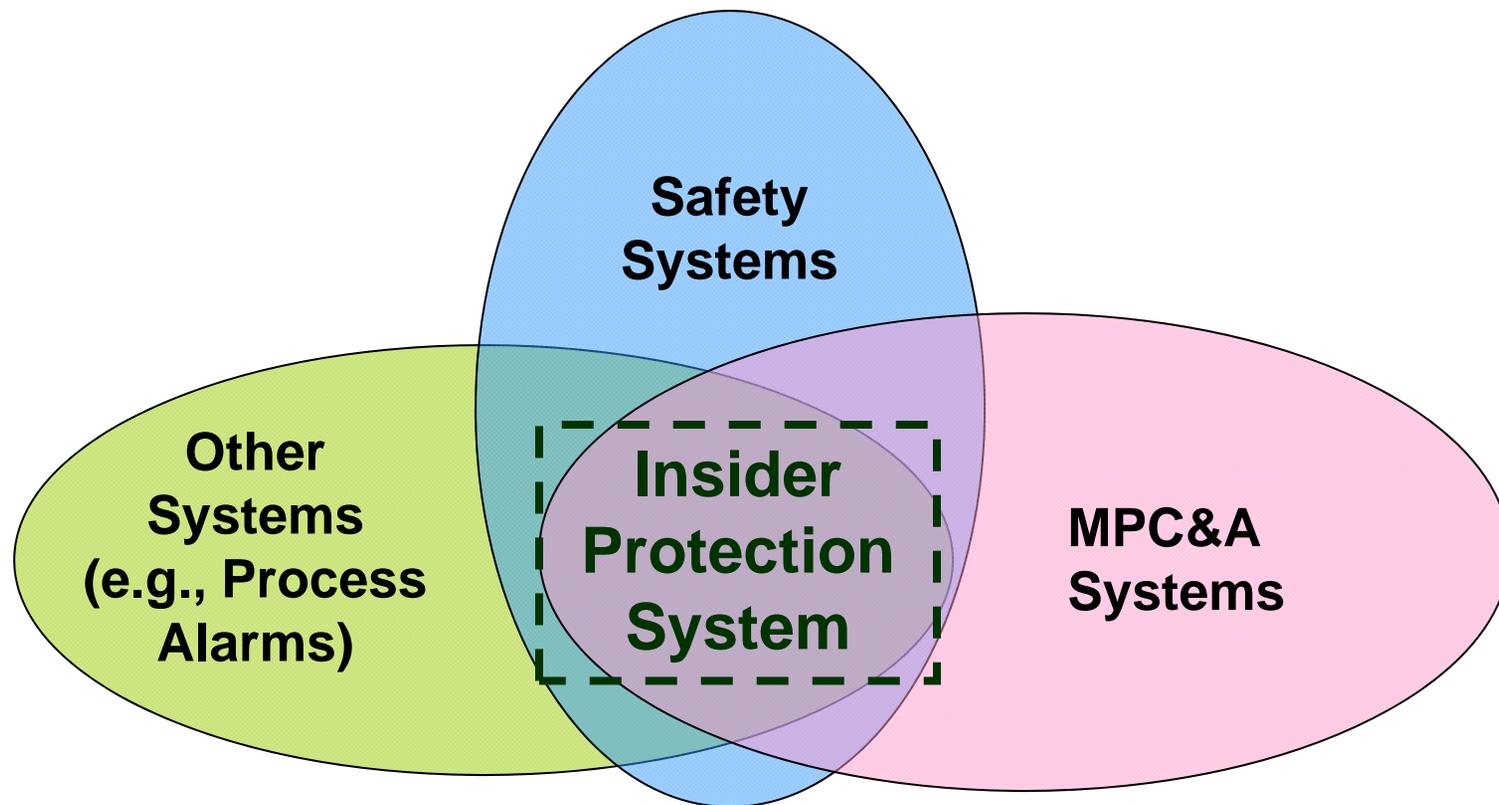
- **Develop and define the insider threat**
- **Identify and characterize the targets**
- **Identify MPC&A technical and administrative measures for insider threat protection**
- **Evaluate effectiveness and relevance of MPC&A measures**
  - **Scenario development**
  - **Analysis**
- **Evaluate effectiveness of overall MPC&A system**
- **Define and evaluate upgraded MPC&A measures**

# Insider Protection System Approach



# Existing Systems Providing Insider Protection

---



# Insiders

---

**Insiders represent formidable threats:**

- they can often circumvent system elements**
- they interact directly with the target without being detected.**

**The delay and detection timelines are not as relevant because insiders can choose the most opportune times and optimum strategies.**

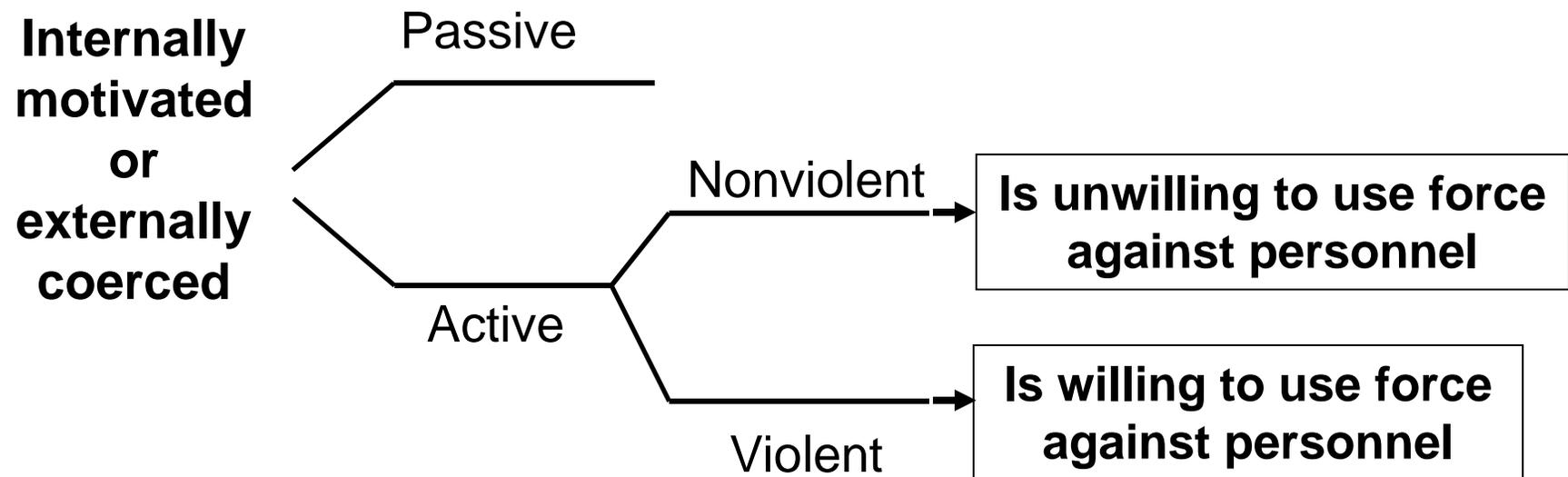
# Insider Definition

---

**Any individual with authorized access to *nuclear facilities or transport* who might attempt unauthorized removal or sabotage, or who could aid *outsiders* to do so.**

- **Insiders might include:**
  - **Management**
  - **Regular employees**
  - **Security personnel**
  - **Service providers**
  - **Visitors**
  - **Inspectors**
  - **Past employees**
  - **Others?**

# Insider Categories



- **All insiders can use stealth and deceit**
- **Violent insiders may be rational or irrational**

# Insider Motivations

---

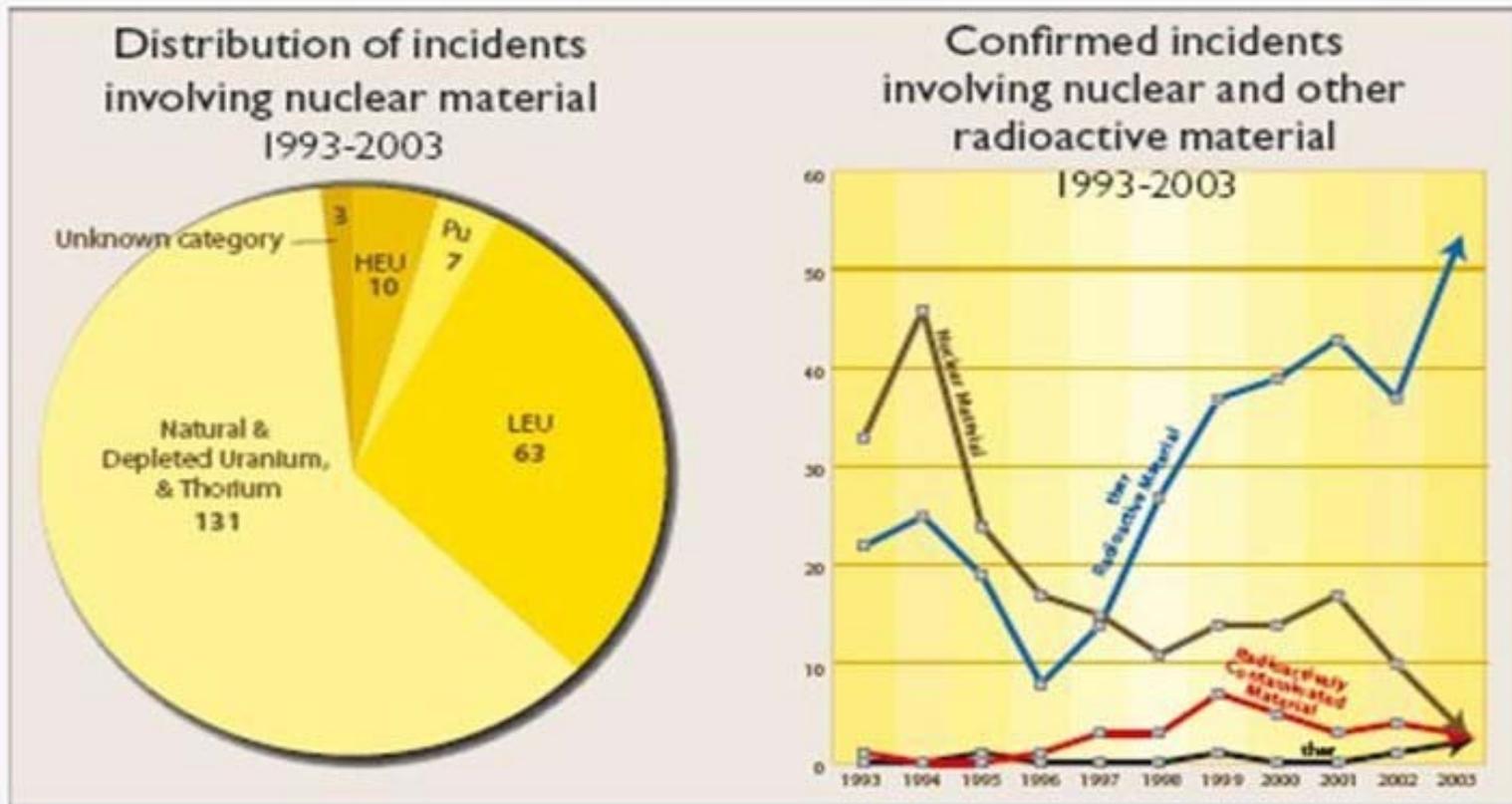
- **Ideological – fanatical conviction**
- **Financial – wants / needs money**
- **Revenge – disgruntled employee or customer**
- **Ego – “look what I am smart enough to do”**
- **Psychotic – mentally unstable but capable**
- **Coercion – family or self threatened**

***Motivation an important indicator for both level of malevolence and likelihood of attempt***

# Trends in Nuclear Trafficking Point to Insiders

Source:

[http://www.iaea.org/Publications/Magazines/Bulletin/Bull461/illicit\\_nuclear\\_trafficking\\_3.html](http://www.iaea.org/Publications/Magazines/Bulletin/Bull461/illicit_nuclear_trafficking_3.html)



# Insider Advantages

---

- **Time**
  - Can select optimum time to implement plan
  - Can extend acts over long periods of time
- **Tools**
  - Has capability to use tools and equipment at work location
  - Can attempt to introduce new tools as necessary
- **Tests**
  - Can test the system with normal “mistakes”
- **Collusion**
  - May recruit / collude with others, either insiders or outsiders

**Insider can exploit these unique capabilities**

# Insider Access

---

- **Authorized work areas**
- **Special temporary access**
- **Escorted or unescorted**
  - **Restrictions on insider during access**
- **Emergency access (fire, medical, police, etc.)**
- **Unauthorized access**
  - **Easy to obtain?**
- **Duration of target exposure**
  - **Conditions of target during insider access**
- **Protection equipment and process tools**
- **Special site equipment**
- **Other?**

# Insider Knowledge

---

- **Targets**
  - Locations, characteristics, and details of targets
  - Details of facility layout
- **Security systems**
  - Security forces capabilities and communications
  - Details of facility and security operations
  - Location and details of safety and security protection systems
- **Operations and processes**
  - Materials accounting
  - Operational processes
  - Tools and equipment
- **Other?**

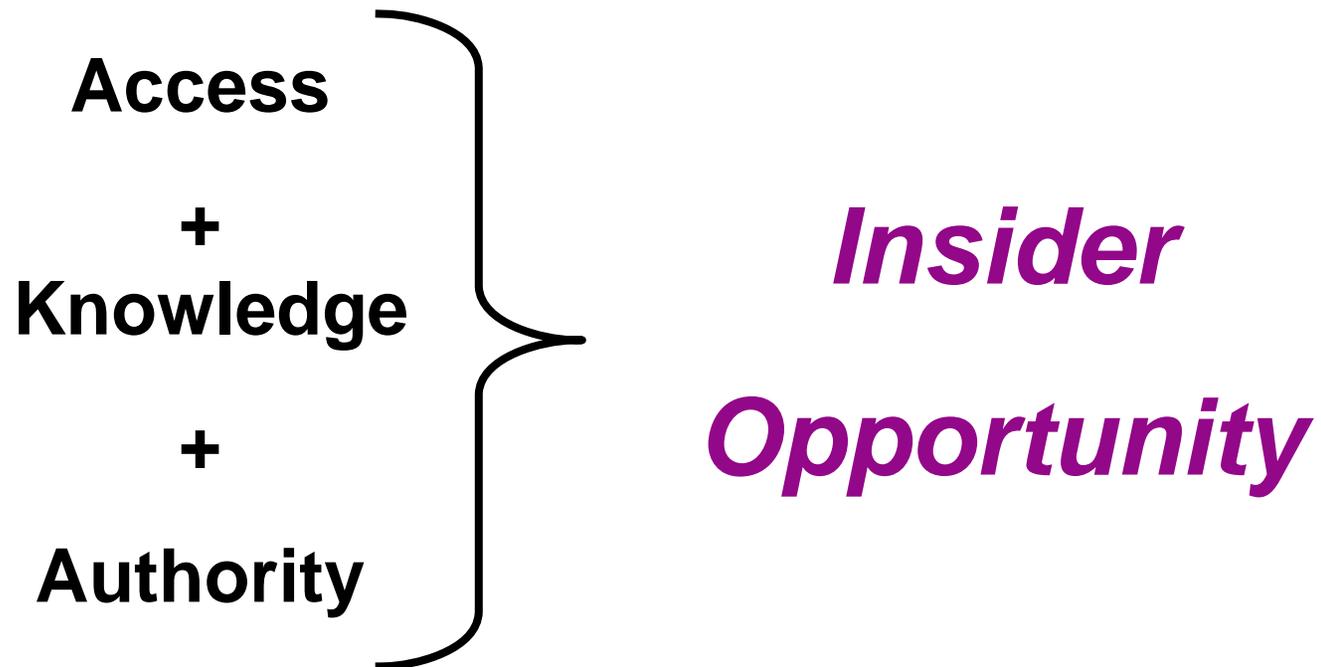
# Insider Authority

---

- **Authority over people**
  - Designated authority over others
  - Personal influence over others
- **Authority over tasks and equipment**
  - Assessment of alarms
  - Preparation of sensitive forms
  - Authorization of processes and procedures
- **Temporary authority?**
- **Falsified authority?**
- **Exemption from procedures?**
- **Other?**

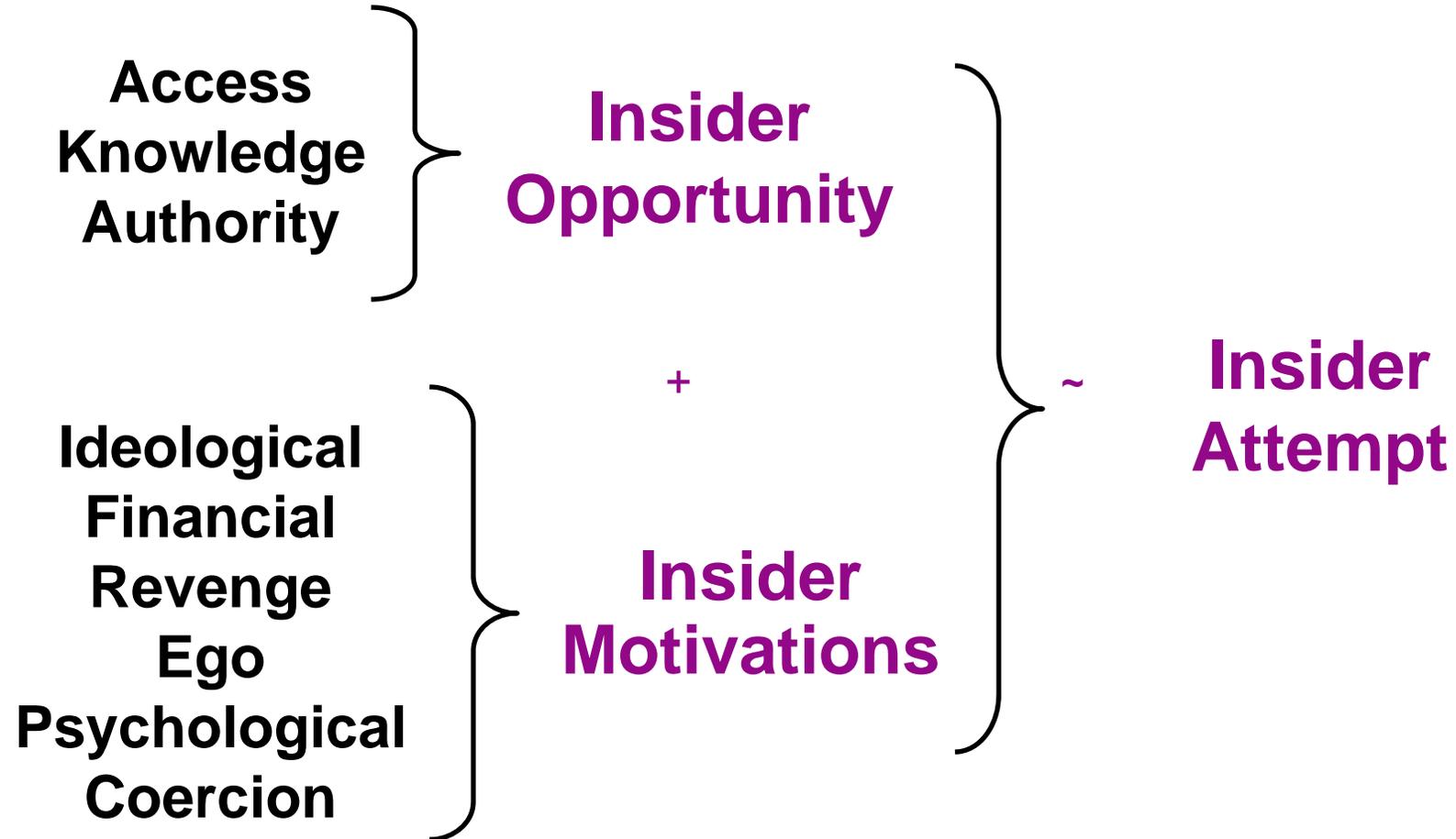
# Opportunity

---



# Factors Affecting Unauthorized Insider Actions

---



# Insider Definition Summary

---

- **Likelihood of unauthorized action**
  - Motivation
  - Opportunity
- **Insider advantages**
  - Time
  - Tools
  - Tests
  - Collusion
- **Facility insider characteristics**
  - Access
  - Authority
  - Knowledge

# Summary - Introductions

---

- **Questions about the course?**
- **Introduction of instructors**
- **Introduction of administrative support/interpreters**
- **Introduction of participants**





# Lecture 2

---

## Hypothetical Facility Overview



# Learning Objective

---

- **Become familiar with the important steps in characterizing a facility**
- **Become familiar with the Hypothetical Facility**
- **Receive briefings and interact with facility management in order to:**
  - **Determine the mission and operations of the facility**
  - **Determine the physical characteristics of the facility**
- **Exercise to review the facility data**

# The Facility Characterization Process

---

- **Philosophy of facility characterization**
  - Document major assumptions underlying VA
  - Be methodical and comprehensive
- **Steps**
  - Gather information
    - Documentation
    - Interviews
  - Obtain or draw facility schematics for analyzing possible adversary paths and target(s)
  - Characterize safeguards and security measures
  - Identify facility states

# Gather information

---

## Sources:

- **Facility tours**
- **Architectural diagrams**
- **Interviews with management and workers**
- **Safeguards and security and material control and accountability plans**
- **Maintenance and operating procedures**
- **Safety analysis reports**
- **Previous vulnerability assessments, audits, surveys, etc.**

# Tour Preparation

---

- **Tour the facility and gather information from interviews**
- **Review schematic diagrams to determine:**
  - **areas,**
  - **protection layers, and**
  - **path elements**
- **For each path element, note safeguards components**
- **Note information on how hardware and procedures are implemented**
- **The system can be characterized at various levels of detail**

# Facility Tour

---

- **Walk-thru of the URF (using diagrams)**
  - **Plant**
  - **Entry Control Building**
  - **Production Facility**
  - **Shipping and Receiving**
  - **Bunker**
  - **Support Buildings**
- **For each path element, note safeguards components**
- **Note information on how hardware and procedures are implemented**
- **The system can be characterized at various levels of detail**

# Interviews with Facility Management

---

- **Overview and Introduction**
  - **Counter Intelligence Officer**
    - **Overview of facility threats**
  - **Facility Manager**
    - **Overview of facility operations**
  - **Materials Manager**
    - **Overview of material operations**
  - **Security Manager**
    - **Overview of security operations**

# Threat Statement

---

- Items were recently confiscated from a political terrorist group's hiding place, which was located less than 200 kilometers from the URF.
- The items included internal engineering drawings of the URF with circles drawn around the Final Products Bunker; various weapons, including automatic weapons; some explosives; and evidence of correspondence and communication with a foreign terrorist group.
- Interviews with property owners and residents indicated the group consisted of three to five men.

# Threat Statement - Continued

---

Intercepted communications from a neighboring country indicates that a large terrorist group has tried to acquire a large quantity of nuclear material.

The local police report that several Special Forces members had been offered large cash payments to provide special training to unidentified individuals.

A major bank robbery was committed in the capital two months ago. Four robbers escaped with a large amount of money. Investigation shows the bank vault was breached by the sophisticated use of high explosives stolen from the local army base.

# Threat Statement - Continued

---

Nationally, many thefts of highly valuable items have occurred. The crimes do not appear to be related to each other. It is speculated that several groups committed the crimes. Organized crime may be involved.

A recent meeting of the Atomic Energy Ministry included a special session on analysis of threat to nuclear facilities and material. No substantiated data on threat were available. However, the general feeling among members was that a threat to nuclear facilities does exist.

During a meeting of the Industrialists Society, concern was expressed by managers of corporations that some of their employees had been approached by unnamed groups to help them carry out theft of valuable equipment and materials from the corporations. The employees had been offered large amounts of money.

# Threat Statement - Continued

---

Two institute employees were recently caught stealing equipment and were terminated from the facility. A new employee drug and competency-screening program was recently introduced.

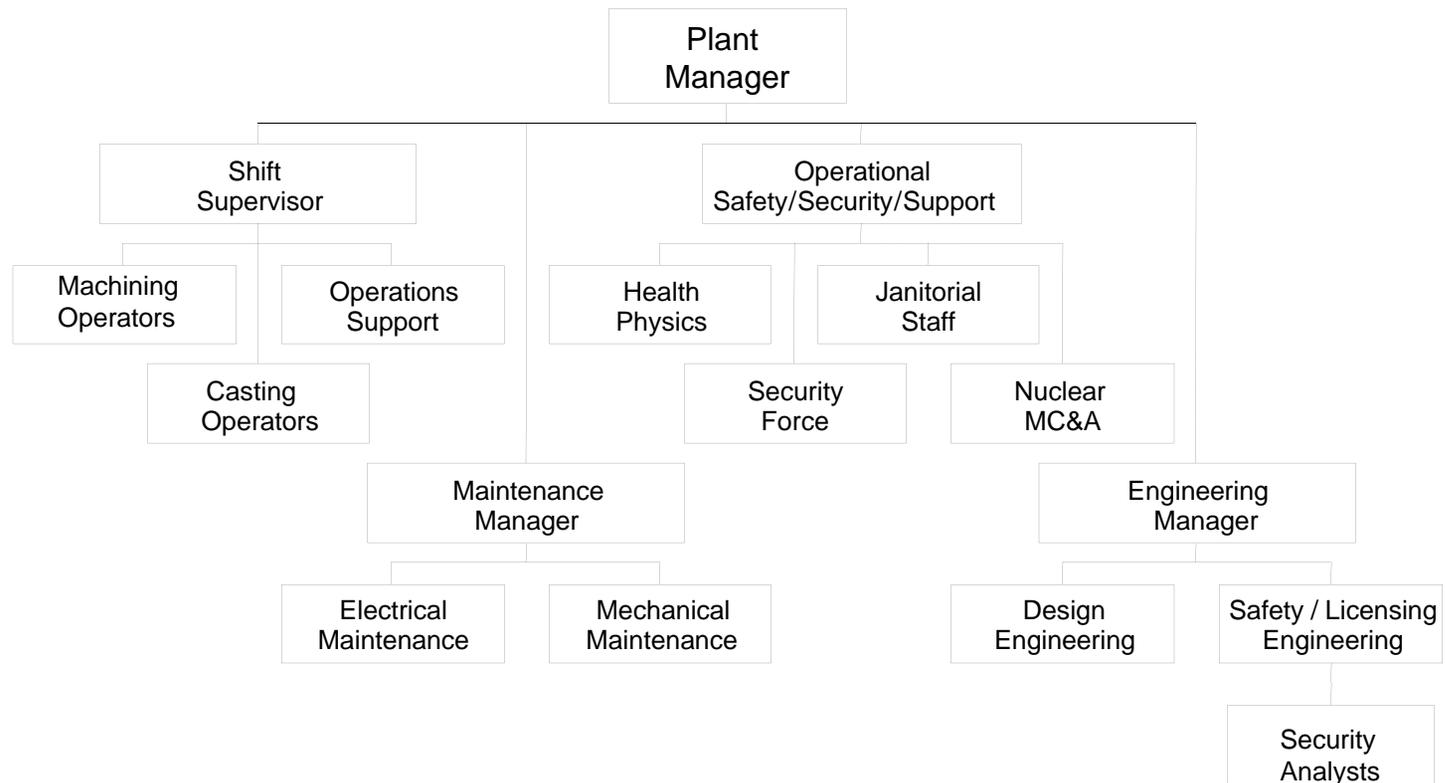
A site-wide inventory recently discovered that several controlled site drawings were missing.

Local reports of upcoming layoffs at the plant have recently been announced in the local news.

The general attitude of the community is tolerant of the URF. However, certain activist groups have protested the plant during religious holidays.

# Interview with Plant Manager

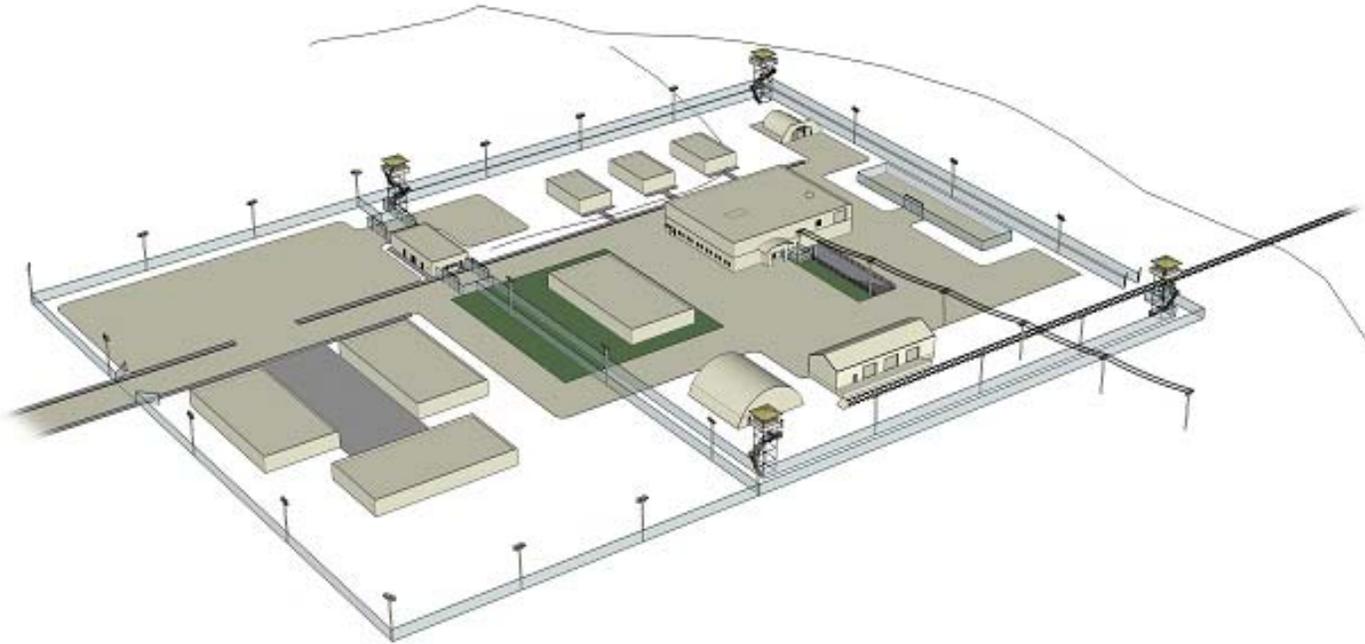
## Overview of facility organization



# Interview with Plant Manager, con't

---

- Overview of facility operations



# Interview with Materials Manager – Overview of Material Operations

| <b>Material Balance Area</b> | <b>Material Form</b>           | <b>Allowable Material Inventory<br/>( kg U, wt % enrich.)</b> |
|------------------------------|--------------------------------|---|
| <b>X-Ray Facility</b>        | <b>Metal billets</b>           | <b>5</b>  |
| <b>Product Bunker</b>        | <b>Metal billets</b>           | <b>300</b>  |
|                              | <b>Oxide powder</b>            | <b>10</b>   |
| <b>Product Bunker</b>        | <b>Metal ingots</b>            | <b>30</b>   |
|                              | <b>Scrap<br/>(all forms)</b>   | <b>50</b>   |
|                              | <b>Metal billets</b>           | <b>20</b>   |
| <b>Analytical Lab</b>        | <b>Samples<br/>(all forms)</b> | <b>3</b>  |

# Interview with Security Manager

- Overview of security operations

| Area                 | Access Controls   | Physical Barriers                                   | Detection Devices                        |
|----------------------|---|---|--|
| AA                   | Employee badge  | Chain-link fence, vehicle gate                      | Guard checks                             |
| PA                   | ECP   | Perimeter Intrusion Detection and Assessment System | Perimeter sensors, tower guards          |
| ECP                  | Employee badge with guard present to ensure correct procedures at metal detectors and SNM detectors | Security doors, walls                               | Guard; metal detectors and SNM detectors |
| X-Ray Facility       | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| Final Product Bunker | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| Production Building  | Entry control portal  | Security doors; walls; guard                        | Metal and SNM detectors                  |
| Product Vault        | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| QA Vault             | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| Chip Vault           | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |
| Casting Furnace Area | 2-person control on locks   | Vault-like construction with Class V doors          | BMS door sensor; interior PIR sensors    |

# Facility Review

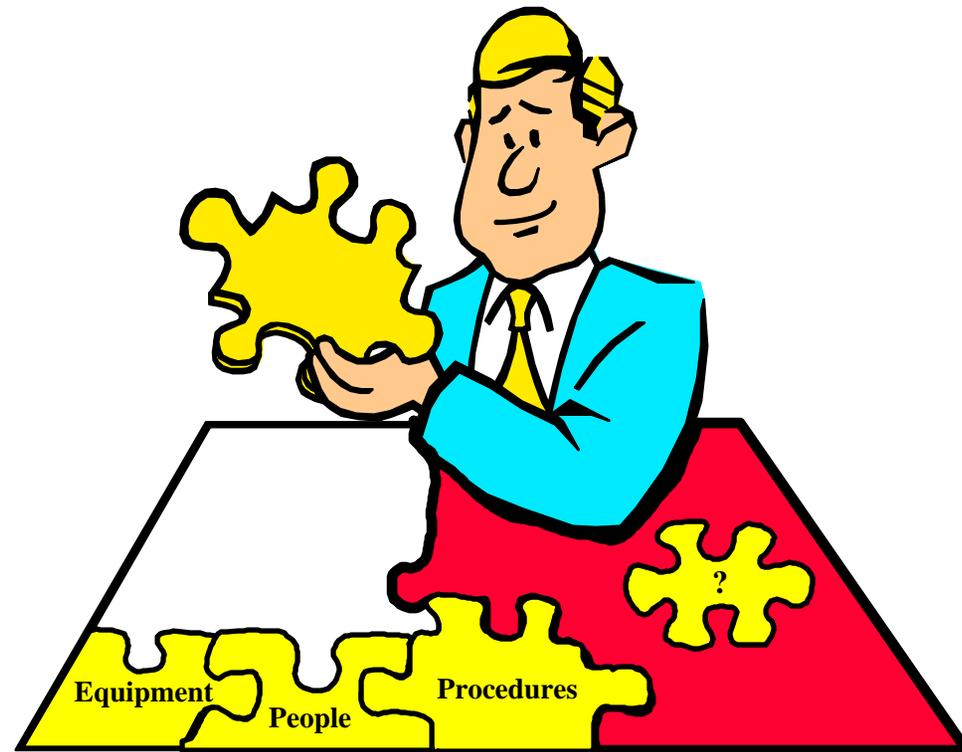
---

- **Comments**
  - **Team 1 Spokesperson**
  - **Team 2 Spokesperson**
  - **Team 3 Spokesperson**
  - **Team 4 Spokesperson**

# Summary

---

- Questions and Answers





# Lecture 3

---

## Personnel Measures

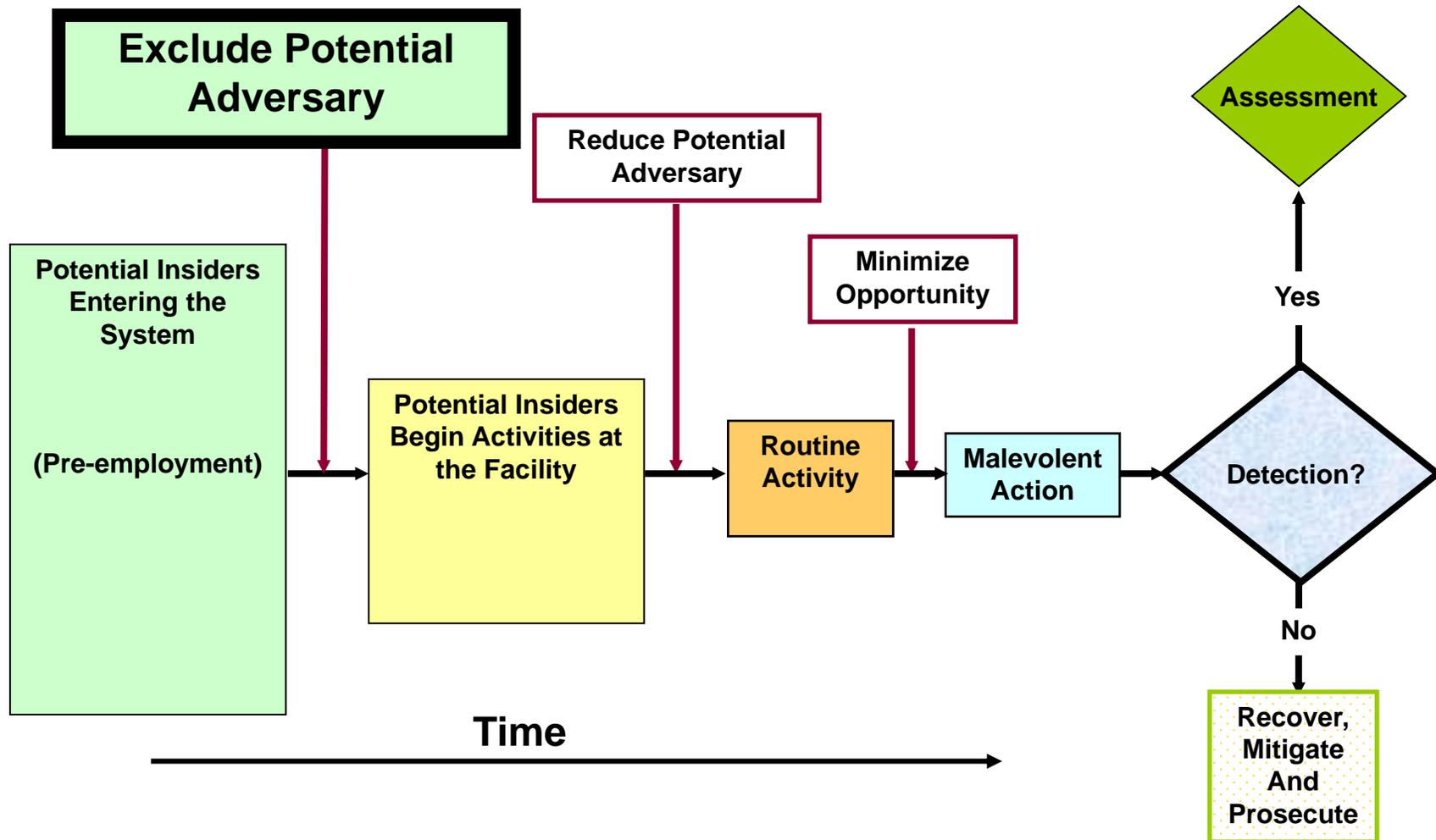


# Learning Objective

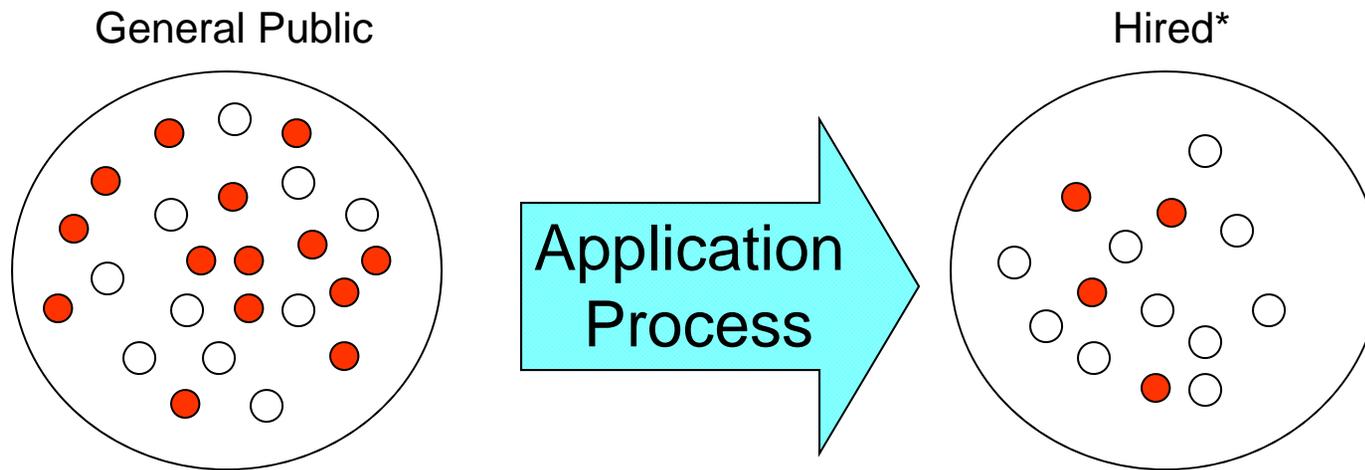
---

- **Review Insider Protection System Approach**
- **Identify administrative measures of an MPC&A system that can provide protection against insider threats**
- **Estimate the effectiveness of administrative measures**

# Insider Protection System Approach



# Exclude Potential Adversaries Based on Undesirable Behaviors



- - persons with desirable behavior
- - persons with undesirable behavior

\* Although these systems are followed ,they are not perfected.

# Exclude Potential Adversary

---

- **Filter potential insiders entering the system**
  - **Pre-employment:**
    - Application process
    - Background checks
    - Financial obligations
    - Work history
    - Other?
  - **Detection (identification) and response (not hiring) can be achieved by the above measures**
  - **Deterrence is also achieved**



# Exclude Potential Adversary: Define Undesirable Behaviors

---

- **Based on your culture, you may define undesirable behaviors as:**
  - **Criminal behavior**
  - **Financial instability**
  - **Substance abuse**
  - **Psychological instability**
  - **Ideology**
  - **Excessive lifestyle**
  - **Others?**
- **Who defines these?**
  - **Management**
  - **State**



# Why Check These Things?

---

- **Malevolent potential may be indicated by criminal history**
- **Financial affairs will provide some indication of stability as well as potential susceptibility to extortion**
- **Work history can reveal tendencies to anger, reliability, mental competency, honesty, etc.**
- **References may reveal information not provided on the application**
  - **Do not limit interviews to only references the applicant provides**

**Note: established criteria will remove many potential employees before activity on-site commences and can serve as cause to terminate employment later on**

# Application Process Example

---

- **Make background check requirements well known to the public**
- **Include a medical examination and substance abuse testing as requirements for certain positions**
- **Ensure that application asks for all information needed to evaluate applicant's behavior**
  - **Financial instability**
  - **Substance abuse**
  - **Psychological instability**
  - **Criminal activity**



# Application Process Example *(cont'd)*

---

- **Post job opening and application acceptance details far enough in advance to allow time for the background checks to be completed before hiring**



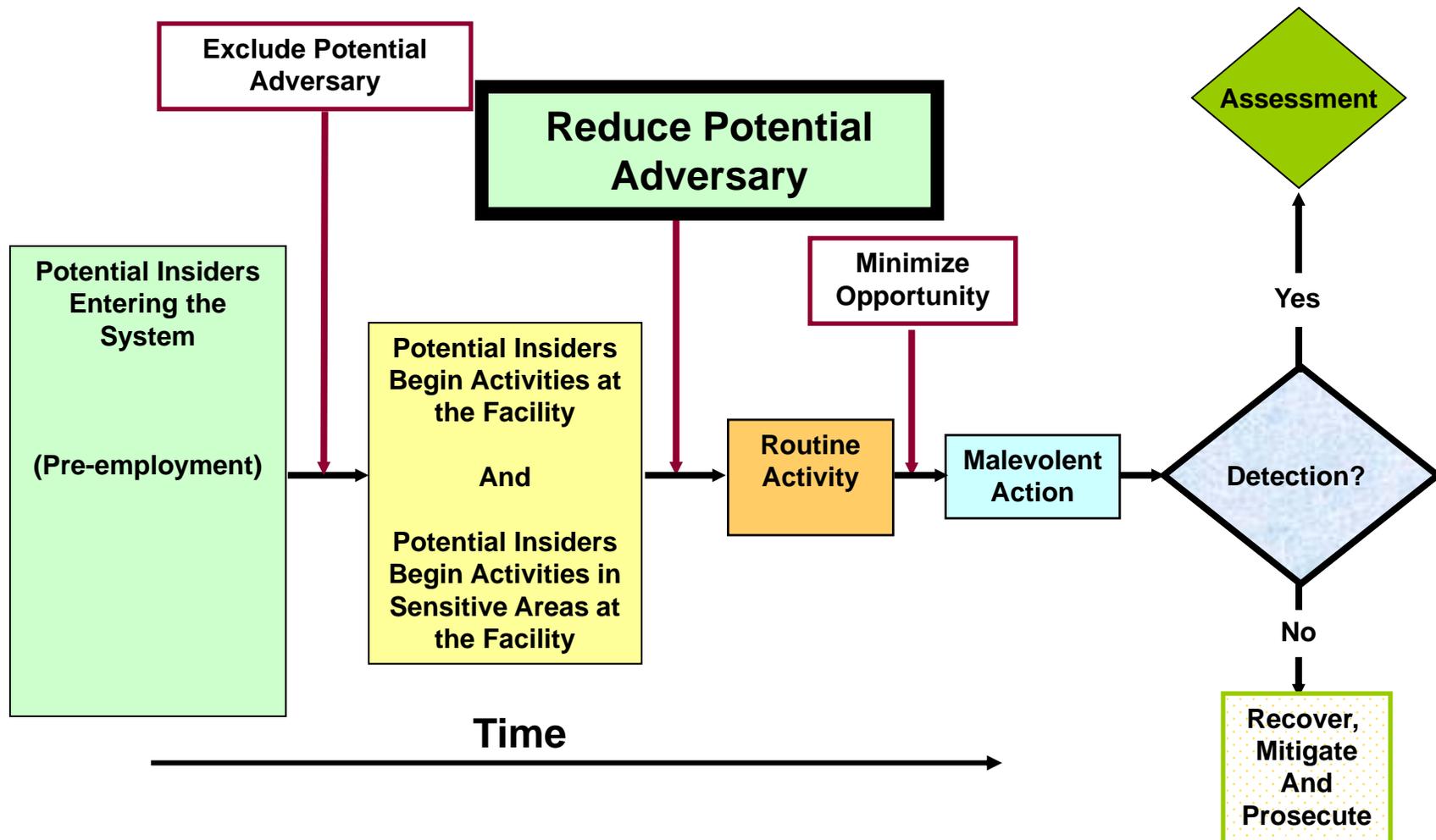
# Background Checks

---

- **There are several levels of checks that are used in various environments – graded approach**
  - **Just the application form and an interview**
  - **A search of national records**
    - **Criminal**
    - **Credit**
  - **A cursory follow-up of the information on the application**
  - **A rigorous follow-up of activity in last several years**
    - **Interview references**
    - **Investigate financial affairs**
    - **Interview previous employers and colleagues**

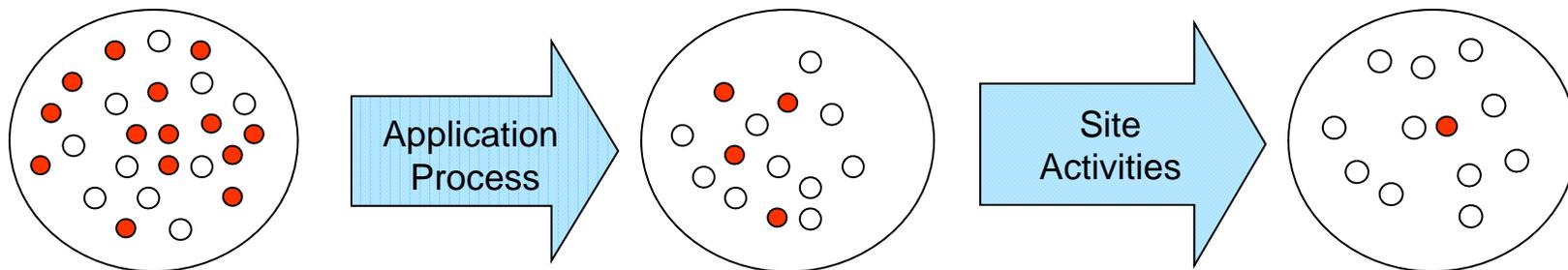


# Insider Protection System Approach



# Further Reduce Potential Adversaries

- Routinely screen employees for undesirable behavior
- Educate employees on correct behavior
- Reward employees for good behavior



- - persons with desirable behavior
- - persons with undesirable behavior

# Reduce Potential Adversary

---

- **For persons who are authorized to conduct activities at the site:**
  - **Periodic re-investigations**
  - **Employee satisfaction program**
  - **Escort & surveillance of infrequent workers and visitor**
  - **Security awareness**
  - **Human Reliability Program (HRP)**
- **Invoke disciplinary action when malevolence occurs**



# Periodic Background Re-investigations

---

- **Similar to the pre-employment check**
- **Emphasis on discovering changes in habits, activities, lifestyle, health, etc.**
- **Perhaps done every 5 years**



# Employee Satisfaction Programs

- **Benefits**
  - Insurance
  - Vacation / holidays
- **Salary treatment**
  - Fairness
- **Working environment**
  - Ergonomics
  - Resources
- **Training**
  - Quality, usefulness, and relevance



# Escort and Surveillance

---

- **Workers such as maintenance, service or construction workers often come from contracting or subcontracting companies**
- **Escorting such people is one way of making sure they are in the right place and they are performing their duties properly.**

# Security Culture/Awareness

---

- **Strong security awareness (Nuclear Security Culture) program for staff and contractors contributes to an ongoing security culture within the organization.**
  - **The purpose of the program is to establish an environment in which all employee are mindful of security policies and procedures, so that they can aid in detection and reporting inappropriate behavior or acts.**

# Mitigate and Prosecute

---

- **Mitigation includes actions that will minimize the consequences (sabotage)**
- **Prosecution**
  - **Provides justice**
  - **Deters others by demonstrating penalties**
  - **Establishes the resolve to address insider problems**
  - **Adjust system to react more favorably based on lessons learned**



# HRP – Human Reliability Program

---

- **Implemented on a graded approach**
- **Usually restricted to persons in job areas which have greater capabilities to commit serious malevolent acts**
- **Includes activities such as frequent drug screening, financial reviews, supervisor and co-worker observation**
- **Frequent physical and mental evaluations**
- **More frequent full background checks**
  - **Perhaps yearly**
- **Supported by a strong security culture**

# Personnel Measures Summary

---

- **Administrative measures used in the insider protection system have the following goals:**
  - **Exclude potential insiders during pre-employment process**
  - **Reduce potential insiders after employment via periodic checks to identify changes in behavior**
  - **Minimize opportunities for malevolent action by insiders**
- **Next step: integrate administrative and technical measures**



# More detail on Human Reliability Program (HRP)

---

- **HRP is a program designed to protect nuclear materials by continuously evaluating employees who work in positions affording unescorted access to those materials**

# Basis of HRP

---

- **Law**
- **Regulations**
- **Executive Orders**
- **DOE orders and manuals**
- **Facility policies and procedures**

# Applicability of HRP

---

- **HRP applies to all individuals who work in positions that allow them access to nuclear materials**
- **These employees must be certified to meet the highest standards of reliability and physical and mental suitability before such access is granted**

# Designating HRP Positions

---

## Criteria for Determining HRP Positions

- **Transportation or protection of special nuclear materials**
- **Knowledge of protective systems for transportation of nuclear materials, explosives, devices, or components**

# General Certification Requirements

---

- **Access authorization (clearance)**
- **Training**
- **Supervisory review, medical assessment, management evaluation, and security review**
- **No history of hallucinogen use in previous 5 years**
- **Psychological evaluation**
- **Drug test**
- **Alcohol test**
- **Initial polygraph examination**

## **Requirements after Certification**

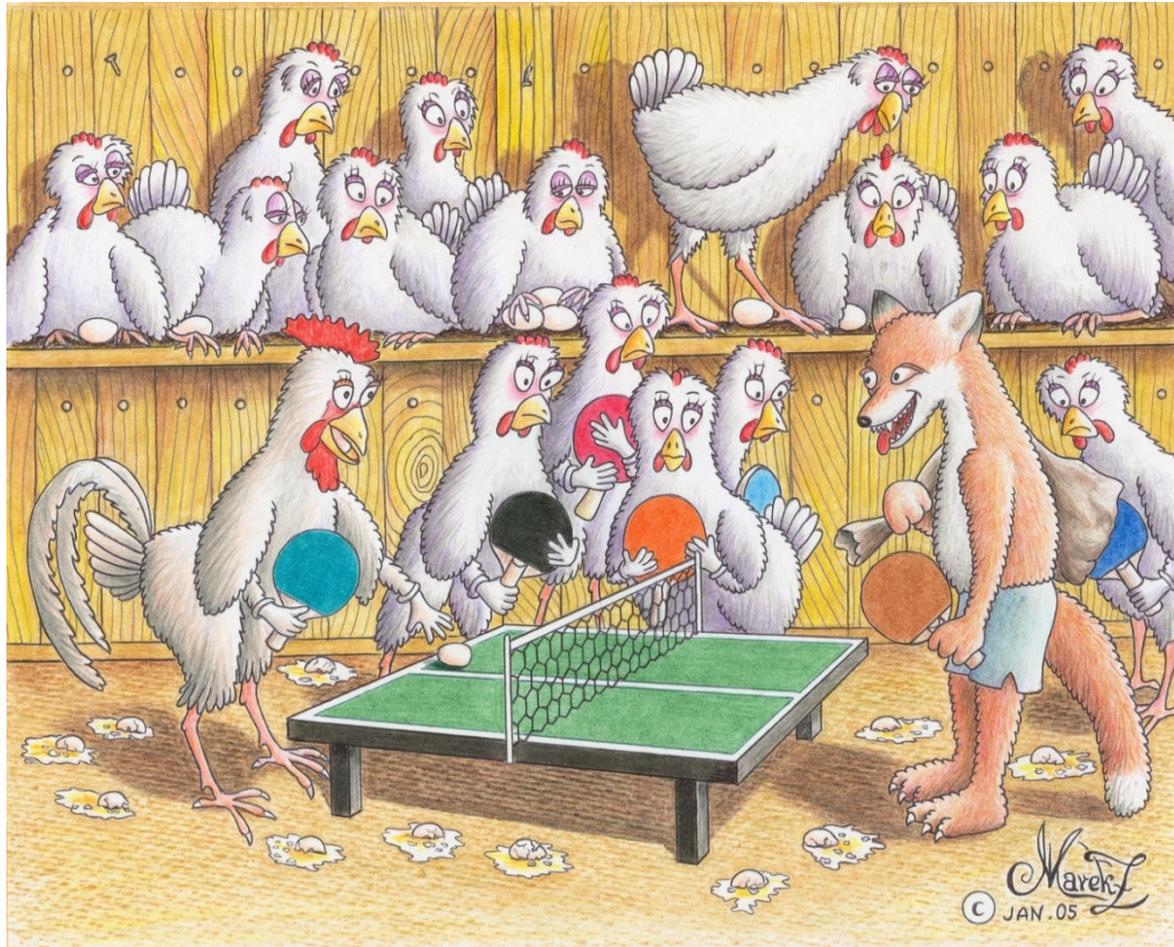
- **Annual training**
- **Annual supervisory review, medical assessment, management evaluation, and security review**
- **Annual psychological evaluation**
- **Drug test (annual, random, for cause)**
- **Alcohol test (annual, random, unannounced, for cause)**

# What are the Benefits of (HRP)?

---

- **Establishes certification standards and requirements for employees in the HRP**
- **Establishes expectations for employees enrolled in the program**
- **Provides stringent continuous evaluation programs designed to identify individuals who may have impaired judgment**
- **Establishes consistent procedures for handling potential problems**
- **Complements physical security upgrades and MPC&A safeguards**

# The Fox Guarding the Hen House (Physical Security Upgrades and MC&A without an HRP)



November 2008

Lecture 3 -27

# How Do I know If It's Working?

---

- **Reduction in incidents involving drugs, alcohol, and workplace violence**
- **Identification of potential problems through continuous evaluations**
- **Absence of incidents related to security of nuclear materials that involve employees in the HRP**
- **Vulnerability assessments that indicate comprehensive “total” safeguards for physical protection, MC&A, and human reliability**

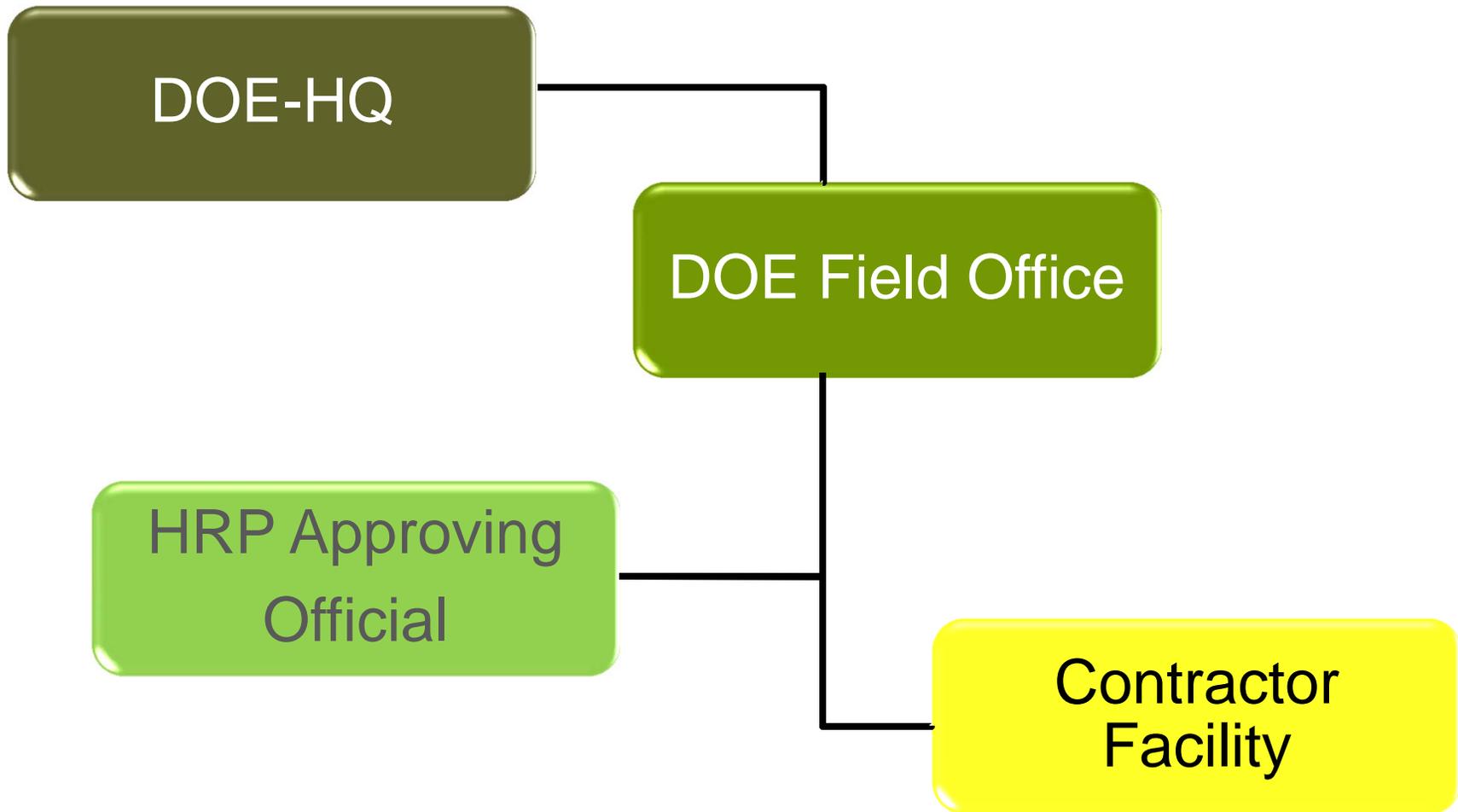
# Evolution of the U.S. HRP (do we need this???)

---

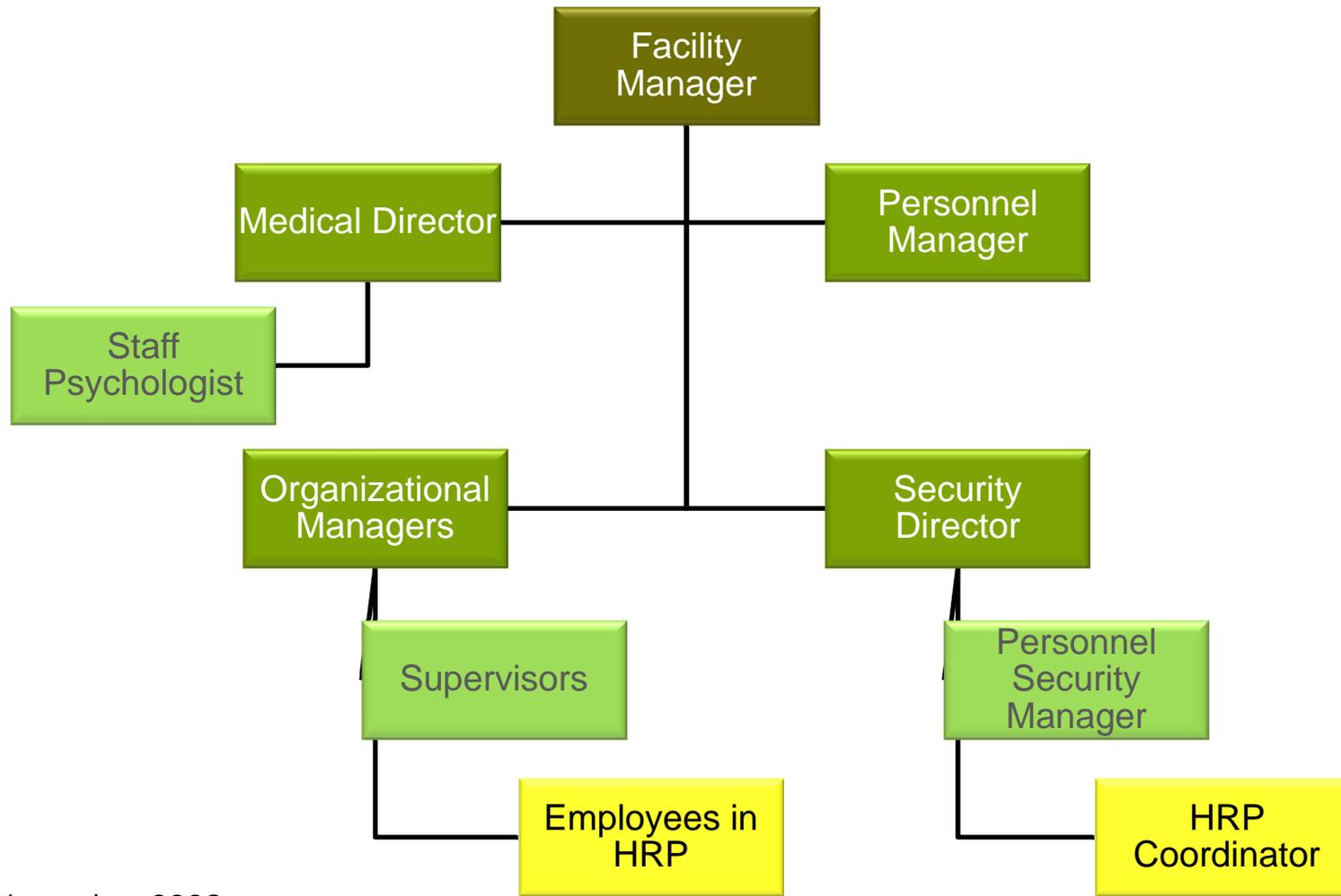
- **Background investigations**
- **Pre-employment drug testing**
- **Personnel Security Assurance Program (PSAP)**
- **Personnel Assurance Program (PAP)**
- **Personnel Reliability Program (PRP)**
- **Human Reliability Program (HRP)**

# HRP Organization

---



# Facility HRP Organization



# Organizational Responsibilities

---

- **DOE-HQ**
  - Establishes HRP Requirements
  - Evaluates requests for access authorization
  - Establishes contractor requirements
- **DOE Field Offices**
  - Provide detailed requirements and procedures
  - Establish objectives, requirements, and responsibilities for contractors
  - Receive and review requests for access to classified matter or material
  - Approve or deny applicants for HRP positions (responsibility of HRP Approving Official)

# Organizational Responsibilities (con't)

---

- ***Site Management:*** Ensures that the facility complies with HRP
  - ***Director of Personnel Resources:*** Ensures that pre-employment checks are completed
  - ***Security Director:*** Formulates policies and procedures, establishes a records management system, and implements the HRP
  - ***Personnel Security Manager:*** Manages HRP
    - **HRP Coordinator:** Schedules HRP activities (testing, training) and maintains records

# Organizational Responsibilities (con't)

---

- ***Medical Director:*** Completes medical assessments and drug/alcohol tests
  - ***Staff Psychologist:*** Performs psychological evaluations and assesses cause of any reported unusual behavior
- ***Organizational Managers:*** Review applicants identified for HRP positions and submit request for approval
  - ***Supervisors:*** Identify applicants for HRP positions
    - ***Employees in HRP:*** Complete paperwork, attend all required training, and keep all scheduled appointments for assessments and evaluations
- ***All Employees:*** Comply with HRP and security requirements and report unusual behavior of any employee to management

# Summary

---

- **Identify verification**
- **Trustworthiness**
- **Employee satisfaction**
- **Escorting and surveillance of works and visitors**
- **Security awareness**
- **Sanctions (disciplinary actions and prosecution)**
- **Human Reliability Program**



# Lecture 4

---

## Administrative Measures



# Learning Objective

---

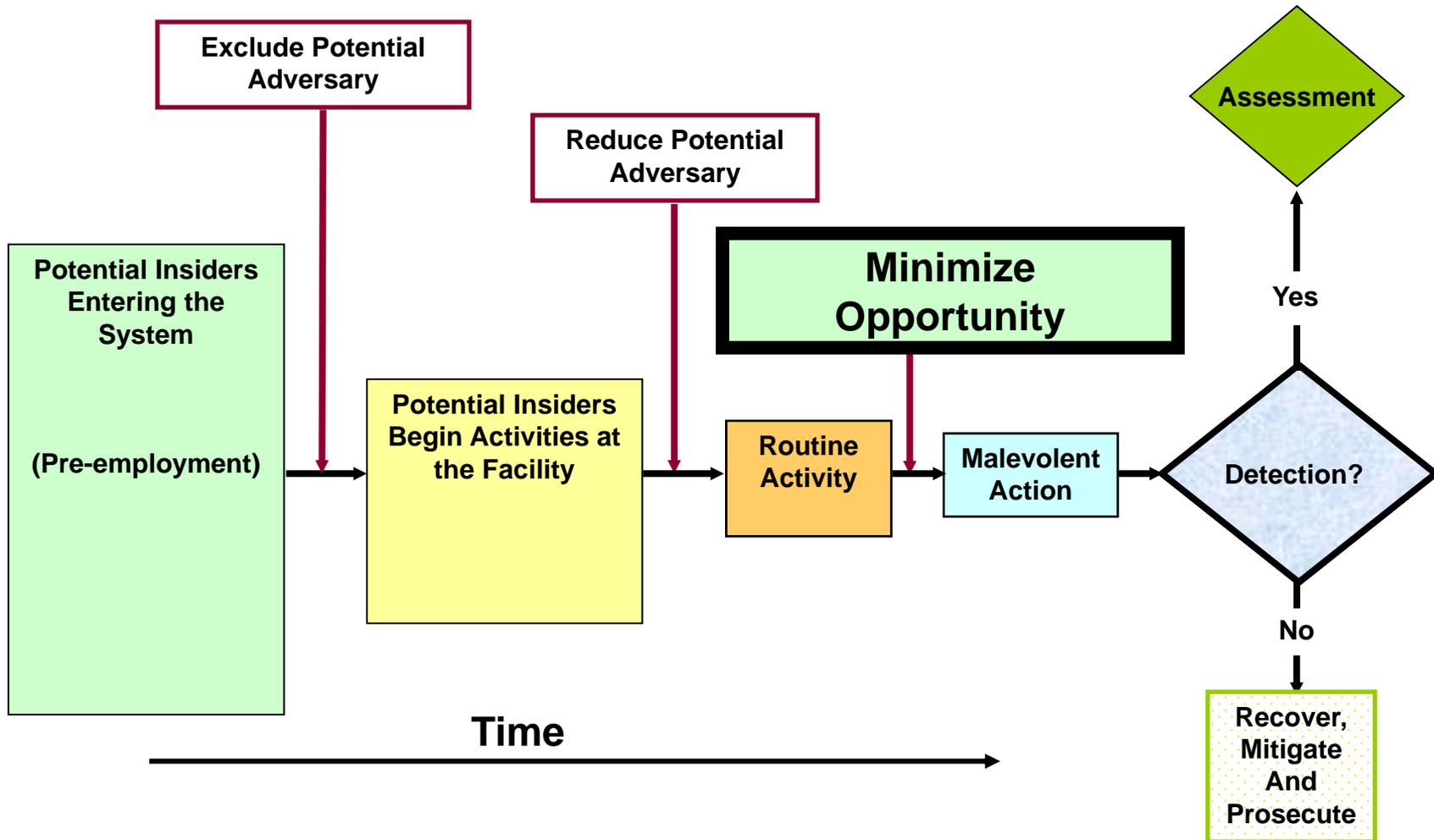
- **Review effective facility operations**
  - **Understand the beneficial coexistence between security and safety**
  - **Understand the mutual benefits between security and material control and accounting elements**
  - **Understand the complimentary nature of other operational activities**
  - **Understand how effective facility operations reduce theft opportunities for the insider**

# Student Learning Objectives

---

- **Review effective facility operations**
  - **Understand the beneficial coexistence between security and safety**
  - **Understand the mutual benefits between security and material control and accounting elements**
  - **Understand the complimentary nature of other operational activities**
  - **Understand how effective facility operations reduce theft opportunities for the insider**

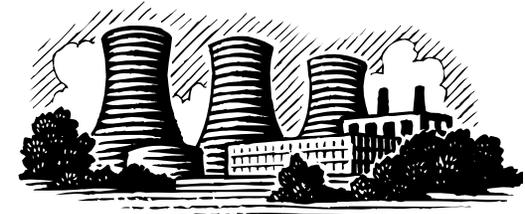
# Insider Protection System Approach



# Minimize Opportunity

---

- **Confidentiality and partitioning of duties and information**
  - **Operational Security Program**
- **Compartmentalize facility**
  - **Access control**
- **Vital equipment operations**
- **Nuclear safety – integrate with security**
- **Inventory management**
- **Quality assurances (QA) programs**
- **Safety and security inspections**
- **Security awareness programs**
- **Materials surveillance**



# Separation of Duties or Functional Independence

---

- **Material accounting should be independent from operations**
  - Prevents operational influence on material accounting personnel.
- **Accounting personnel should not have routine access to material**
  - Reduces capability to conceal unauthorized activities
- **Separation of duties among MC&A functions**
  - Reduces possibility of hiding unauthorized activities
  - System of checks and balances

# Confidentiality and Compartmentalization of Information

---

- **Limit information available to each person that is needed to do the job**
  - **Need to know**
- **Separate information to prevent full knowledge of sensitive areas**
- **Information of concern**
  - **Location and condition of sensitive targets**
  - **Details of preventive and protective systems**
  - **Critical elements of system design**
  - **Vulnerabilities in the system**



# Confidentiality and Compartmentalization of Information *(cont'd)*

---

- **Classified or restricted data**
  - Based on a state definition of what is sensitive information
  - Could also be company proprietary
- **Operational security program**
  - Shipment data, organizational lists, etc.



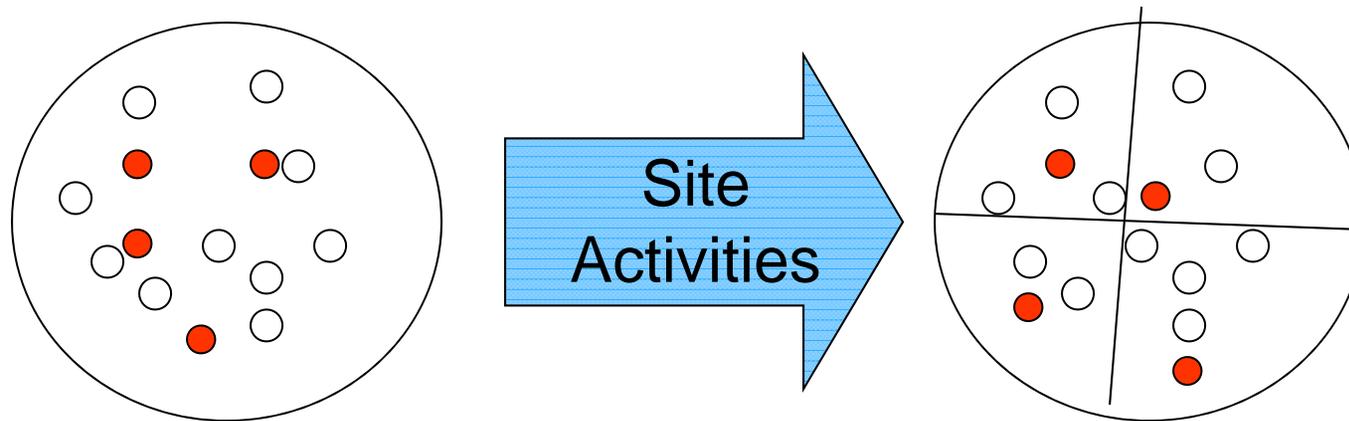
# Records and Reports

---

- **Limit access and authority to the accounting system**
  - Reduces opportunity for insiders to change accounting records
- **Accounting values based on measurements**
  - Ensures accuracy in the accounting records
- **Quality assurance of input data**
  - Reduces probability that insiders can introduce false data into the accounting records
- **Complete audit trail**
  - Increases probability that false or erroneous information can be indentified and corrected

# Further Reduce Potential Adversaries

- **Compartmented activities further reduce potential insiders**



- - persons with desirable behavior
- - persons with undesirable behavior

# Administrative Compartmentalization of Facility

- **Authorize access to nuclear materials and sensitive areas of the facility to:**
  - **Restrict access to those needing it for job duties**
    - **Location and time**
  - **Allow access to only part of the equipment needed to complete a successful theft or diversion**
  - **Incorporate monitoring activities to detect potential malevolence and determine who is responsible for such acts**
  - **Separate duties**
    - **Limit access and authority**
  - **Enforce two-person rule in vital areas**



# Vital Equipment Operations

---

- **Preventive and corrective maintenance**
  - Under controlled conditions
- **Escort maintenance personnel**
  - Provides oversight
- **Inspect and test after equipment has been accessed or maintained**
- **Daily tests ensure operability**
- **Protect spare parts by security or separation**



# Nuclear Safety

---

- **Criticality concerns**
- **Personnel safety issues**
- **Safety criteria and/or layout criteria are established for important systems or equipment**
  - **Safety criteria: redundancy, technology diversification**
  - **Layout criteria: physical or geographical separation**
- **Margins of safety are included to be able to cope with abnormal situations and severe sequences of events**



# Health and Safety Elements

- **Criticality safety alarms**
- **Radiation monitors**
- **Contamination surveys**
- **Emergency evacuation procedures**
- **Safety and Security may complement or each other**
  - **Process monitoring, criticality limits**
  - **Evacuations**



# Operational Process Alarms

---

- **Monitor normal operational process / safety alarms for abnormal conditions**
- **Alarm on sensor threshold violations or equipment failures**
- **Alarms can trigger automatic actions or alert operators to take action**



# Inventory Management – Reduced Inventory

---

- **Reduced inventory**
  - **Restricts the amount of material available for theft or radiological dispersal**
  - **Supports material accountancy since less material is present at any location**
  - **Consolidation may reduce insider access to materials**
    - **May also increase risk by providing a more attractive target**
  - **Floor limits**



# Inventory Management – Materials Accounting

---

- **Materials accounting**
  - **Accounting provides material traceability**
  - **Inventory verifies**
    - **Material location**
    - **Type**
    - **Amount**
  - **Measurements confirm material type and quantity**
  - **Transfer control maintains integrity between system elements**



# Security Awareness Program

---

- A program intended to remind employees of their security roles and responsibilities
- Usually part of routine frequent employee training
- Sensitizes employees to watch for and report or interfere with potential malevolent actions
- Spans the spectrum of concerns
  - Cyber, physical protection, MC&A, information, etc.
- A product of a strong security culture



# Quality Assurance Programs

---

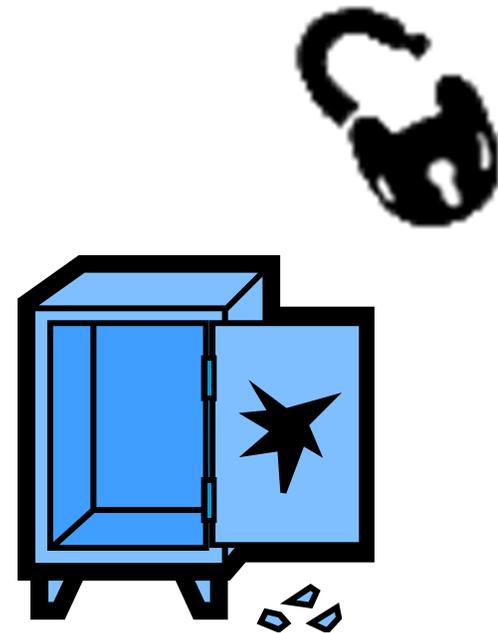
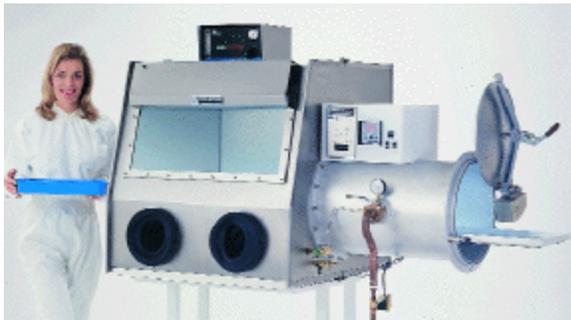
- **Quality management system should include:**
  - **Process monitoring**
  - **Performance testing**
  - **Procedure compliance**
- **Provides traceability**
- **Quality records**
  - **Example: verify compliance to the two-person rule by observing the actual actions of the personnel involved and monitoring the associated quality records**



# Administrative Checks

---

- Can detect compromises of equipment or unusual conditions
- Example
  - Inspection inventory in glove boxes



# Daily Administrative Checks (DAC)

*(continued)*

---

- **Provide timely detection of obvious anomalies**
- **Facility specific check lists**
- **Health, Safety, and Radiation Protection**
  - **Storage location observations**
  - **Equipment (Gloveboxes, open containers)**
  - **Observing material movements**

# Example DAC (continued)

REVISION 2  
Page 2 of 3

## DAILY ADMINISTRATIVE CHECK

| AREA                 | TIME | VERIFICATION TASK | INSPECTION RESULTS           |                                |                              |
|----------------------|------|-------------------|------------------------------|--------------------------------|------------------------------|
| <b>MBA 1375-01</b>   |      |                   |                              |                                |                              |
| Vault 1101           |      | Outer Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Inner Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Door Integrity    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Alarm Systems     | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| Vault 1208           |      | Outer Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Inner Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Door Integrity    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Alarm Systems     | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| <b>1375-30</b>       |      |                   |                              |                                |                              |
| Room 3602<br>WCGE    |      | Door Integrity    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| <b>MBA 1375-31</b>   |      |                   |                              |                                |                              |
| Vault 3331           |      | Outer Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Inner Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Door Integrity    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Alarm Systems     | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| <b>MBA 1375-38</b>   |      |                   |                              |                                |                              |
| Room 1103            |      | Tank (s) Volume   | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Tank Integrity    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| <b>MBA 1375-45</b>   |      |                   |                              |                                |                              |
| Multiplicity Counter |      | Items located     | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| Room 3541            |      | TIDs Intact       | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| <b>MBA 1375-49</b>   |      |                   |                              |                                |                              |
| Vault 3337           |      | Outer Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Inner Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Door Integrity    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Alarm Systems     | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| <b>MBA 1375-50</b>   |      |                   |                              |                                |                              |
| Vault 3606           |      | Outer Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Inner Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Door Integrity    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                      |      | Alarm Systems     | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |

REVISION 2  
Page 2 of 3

## DAILY ADMINISTRATIVE CHECK (continued)

| AREA                           | TIME | VERIFICATION TASK | INSPECTION RESULTS           |                                |                              |
|--------------------------------|------|-------------------|------------------------------|--------------------------------|------------------------------|
| <b>MBA 1375-50 (continued)</b> |      |                   |                              |                                |                              |
| Vault 3327                     |      | Outer Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                                |      | Inner Surfaces    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                                |      | Door Integrity    | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
|                                |      | Alarm Systems     | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| <b>MBA 1375-70</b>             |      |                   |                              |                                |                              |
| Stacker/Retriever              |      |                   | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| Windows in Sub Basement        |      |                   | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| Walls                          |      |                   | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| Doors                          |      |                   | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| Stairwell #1                   |      |                   | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| <b>MST Teams</b>               |      |                   |                              |                                |                              |
| 2 person rule                  |      |                   | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |
| Radio compliance               |      |                   | <input type="checkbox"/> SAT | <input type="checkbox"/> UNSAT | <input type="checkbox"/> N/A |

Comments: \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

Performed By: \_\_\_\_\_ / \_\_\_\_\_  
 NMC Personnel / Date

- Deficiencies identified and submitted to Building Management
- No deficiencies

Reviewed By: \_\_\_\_\_ / \_\_\_\_\_  
 NMC Building Lead / Date

**NOTE:** This document is unclassified unless a unsatisfactory mark is indicated. Protect document as "Confidential" and have reviewed for classification **immediately** if this occurs.



# Lecture 4.1

## Two Person Rule



# Purpose of the Two-Person Rule

---

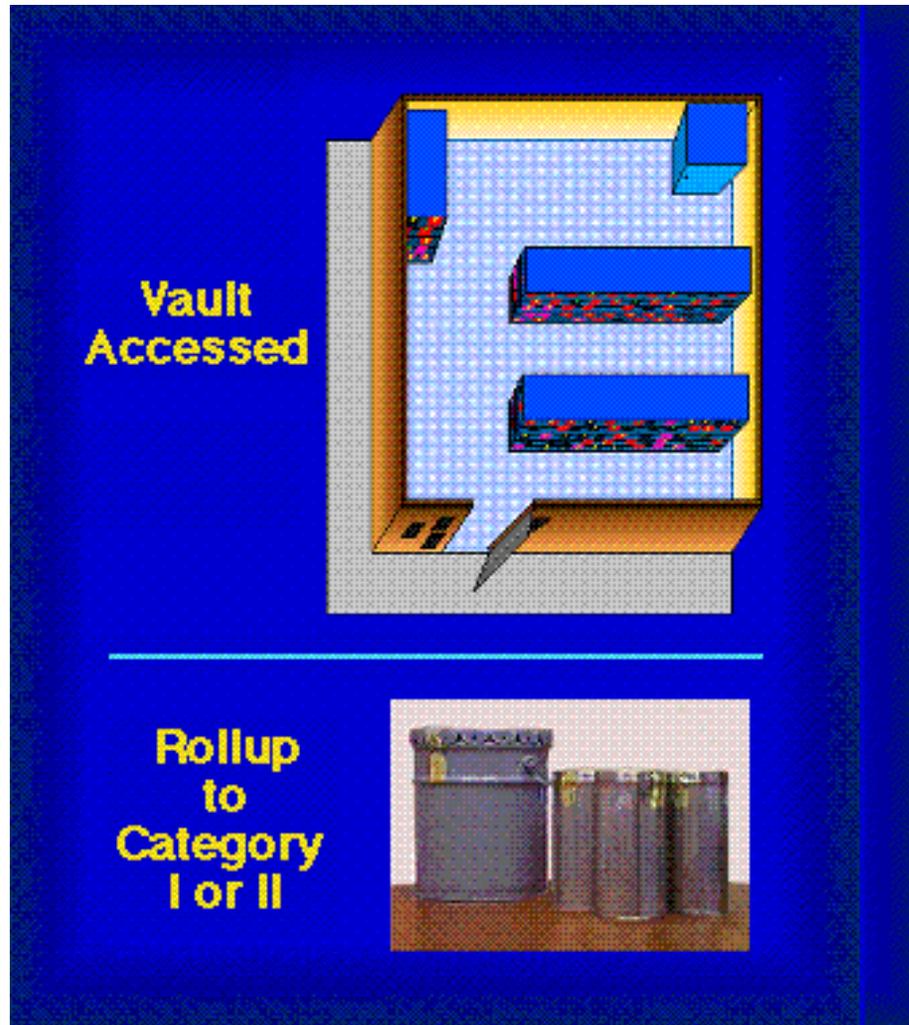
- **The primary purpose of the Two-Person Rule is to ensure that no single individual is in a position to divert, remove, or sabotage special nuclear material without timely detection.**
- **This single individual or insider threat can be any person currently working within your facility or a person not directly related to day-to-day operations.**

# **When to Apply the Two-Person Rule**

**The Two-Person Rule must be used when personnel have access to quantities of SNM and:**

- the material is NOT protected by an active security alarm system or other material surveillance mechanisms.**
- smaller quantities of material can be easily accumulated into a Category I or II quantity.**

# Examples



November 2008

Lecture 4 -26  
Lecture 3 Targets - 26

# When to Apply the Two-Person Rule

(cont'd)

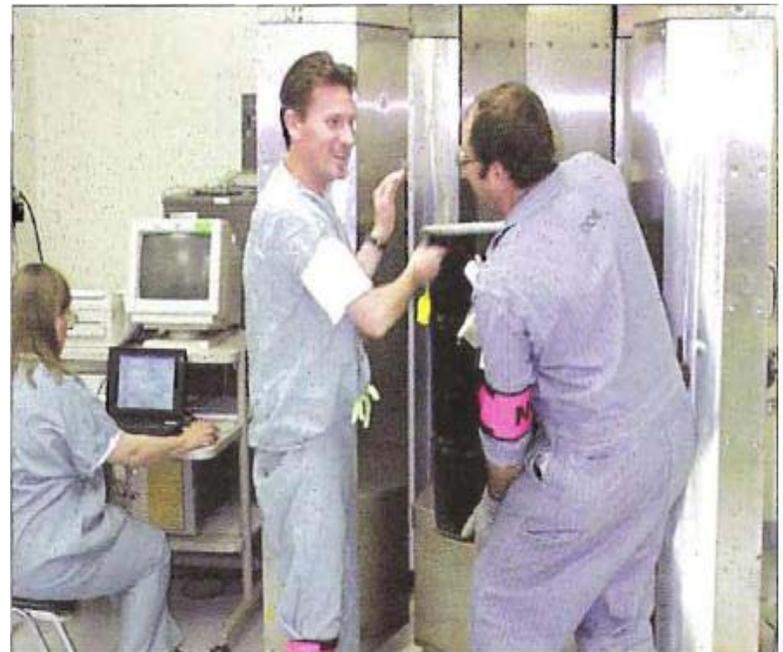
---

- **The application of the Two-Person Rule can be associated with a wide assortment of conditions in the facility. These conditions can include SNM production, packaging, measurements, material transfers, and SNM not under secured storage conditions.**
- **Routine facility maintenance of general access into areas where these quantities of SNM are located would also require the application of the Two-Person Rule.**

# Principles to Follow

There are three basic principles that must be followed at all times when participating as part of a Two-Person Rule team:

- Clearly observe each other at all times
- Observe the special nuclear material or access to that material
- When accessed, at least one member of the Two-Person Rule team must observe the entrance to storage areas



## **Principles to Follow** (cont'd)

---

- **If any work in the facility where a Two-Person Rule is required cannot meet these requirements, work must be stopped and unobservable workers must exit the area.**
- **All outside visitors must be observed by a Two-Person Rule team. Depending on the size of the group, this task may require more than two people.**
- **Documentation of the Two-Person Rule participants is required when used. Procedures or log sheets may be used to document compliance with the Two-Person Rule.**

# Requirements for a Two-Person Rule Participants

Each person must meet all of the following requirements before they can be part of a Two-Person Rule Team:

- Properly cleared for the category and amount of special nuclear material being controlled
- Knowledgeable of correct facility procedures
- Authorized to be part of the Two-Person Rule
- Complete the required Two-Person Rule training



# Locations for Two-Person Rule Application

---

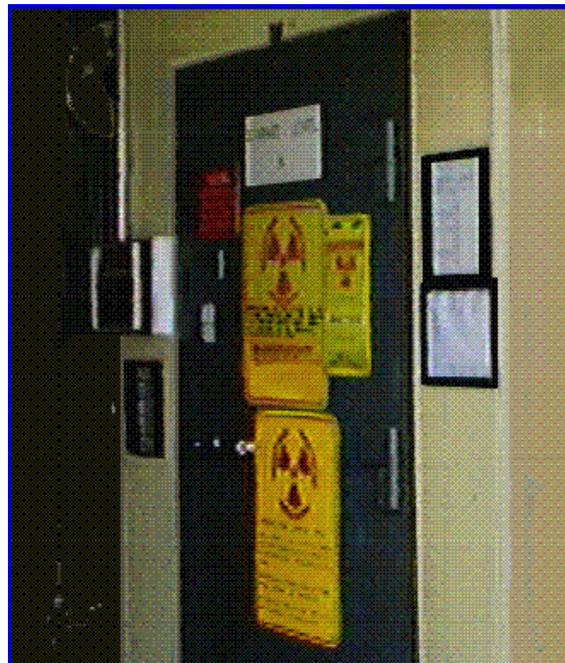
There are certain areas where the Two-Person Rule must be applied. These areas include:

- **Secure storage areas**
- **Process lines with Category I or II quantities of SNM**
- **Areas with high sabotage potential**
- **Safeguards and security systems**
- **Material transfers across MAA boundaries of Category I and II SNM items**

# Locations for Two-Person Rule Application (cont'd)

## Secure Storage Areas

- **Secure storage areas include storage areas used for the storage of Category I and II quantities of SNM. There are several Two-Person Rule requirements that must be followed for these areas.**



# Locations for Two-Person Rule

## Application (cont'd)

### Secure Storage Areas (cont'd)

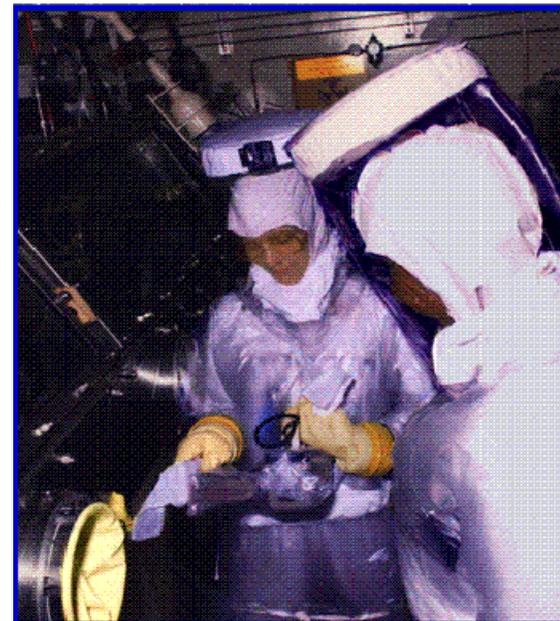
---

- **Upon Entry into a secured storage area, personnel must:**
  - **Have access authorization checked**
  - **A minimum of two authorized persons are required to enter storage area**
  - **Be capable of clearly observing each other at all times**
  - **Be capable of observing SNM or access to SNM**
  - **Have constant observation of entrance (by at least 1 team member)**
  - **Additional persons may need to be added to the two-person rule surveillance team in order to accomplish all of the above tasks and complete the assigned work in the storage area.**

# Locations for Two-Person Rule Application (cont'd)

## Process Line

- **Process lines or production areas that have Category I and II quantities of SNM and are accessible by personnel in the work area require the application of the Two-Person Rule.**
- **These manufacturing areas can include chemical/mechanical processing lines, glove boxes, maintenance aisles, huts, repackaging areas, and assay areas.**



# Locations for Two-Person Rule Application (cont'd)

## Process Line (cont'd)

---

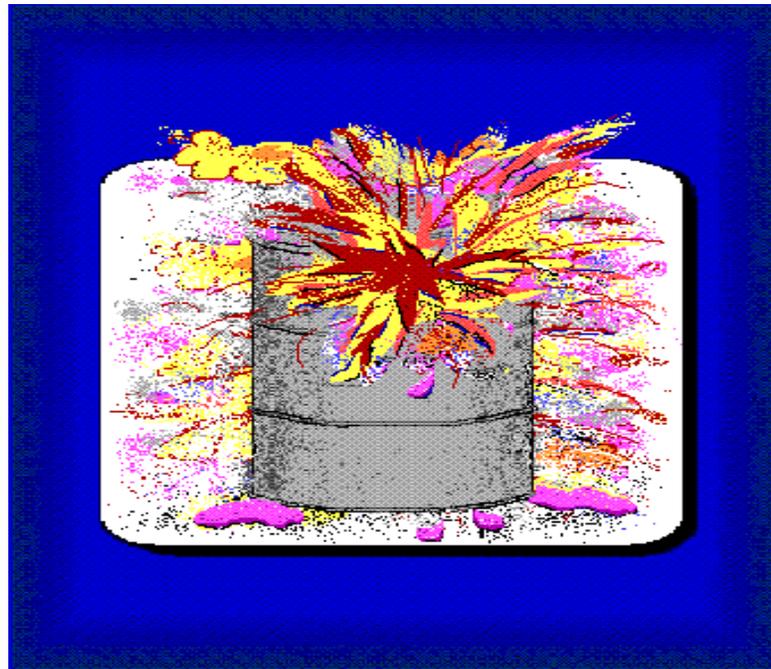
- **Since process area entries are in a storage area, watching those entries is NOT required. However, it is the responsibility of the persons entering the area to comply with the Two-Person Rule requirements upon entry.**
- **One person can be assigned to watch several other workers as long as all Two-Person Rule requirements are met.**

# Locations for Two-Person Rule Application (cont'd)

## Sabotage Potential

---

- A Two-Person Rule is required in all areas where sabotage risks are designated as “High”.
- All personnel must be alert for the potential sabotage of SNM and the production of SNM.



# Locations for Two-Person Rule Application (cont'd)

## Safeguards and Security Systems

- **Key safeguards and security systems can include portal monitors, classified computer systems, and access control systems where SNM is located. Required maintenance on these systems must be performed by a two-person team. Both members must be knowledgeable of work being performed on the safeguards and security system.**



# Locations for Two-Person Rule Application (cont'd)

## Material Transfers Across Material Access Area Boundary

---

- **A Two-Person Rule is required to transfer all radioactive materials out of a Material Access Area (MAA). Radioactive material includes all accountable nuclear material (e.g., HP sources, technical standards, process samples). These types of items can set off a portal monitor alarm upon being checked at the MAA boundary.**

# Locations for Two-Person Rule

## Application (cont'd)

### Material Transfers Across Material Access Area Boundary (cont'd)

---

- Any person who signs to authorize a nuclear material transfer cannot be part of the Two-Person Rule team carrying the material out of the MAA.
- Transfer documentation and authorization prior to releasing the material for MAA are required.
- The protective force at the MAA boundary checks for adherence of the Two-Person Rule requirement for transferring radioactive material out of the MAA.

# Tamper Indicating Program

---

- **A device that may be used on items such as containers and doors, which because of its uniqueness in design or structure reveals violations of container integrity.**
- **Or Simply - Devices that indicate, upon proper inspection, whether tampering or entry has occurred.**

# Tamper Indicating Program

---

- **The use of two authorized TID Applicators protects against a single person diverting or substituting material being placed in a storage or shipping container. Both persons are responsible for ensuring that the correct material is placed in the container prior to the application of the TID seal. Both persons are also responsible for ensuring the seal is applied correctly and is intact (integrity).**

# Tamper Indicating Program (cont'd)

---

- The application, removal, and destruction of TIDs require the use of two authorized TID Applicators.



November 2008

Lecture 4 -42

Lecture 3 Targets - 42

# Nuclear Material Physical Inventories

---

- A Two Person inventory team is used to ensure the validity of information collected during a physical inventory.



November 2008

Lecture 4 -43

Lecture 3 Targets - 43

# Nuclear Material Physical Inventories

(cont'd)

---

- **Physical inventories are taken for each material balance area (MBA) in order to obtain an accurate accounting of the nuclear material that is present in the facility.**
- **Two-person inventory teams systematically search through the entire facility to physically locate all nuclear material.**

# Other Uses of Two Person Teams

---

- **There are other activities which require the use of two person teams, where it is not necessary for those persons to be Two-Person Rule qualified. For instance, TID application and inventories for any Category of material or any reason require two person teams.**

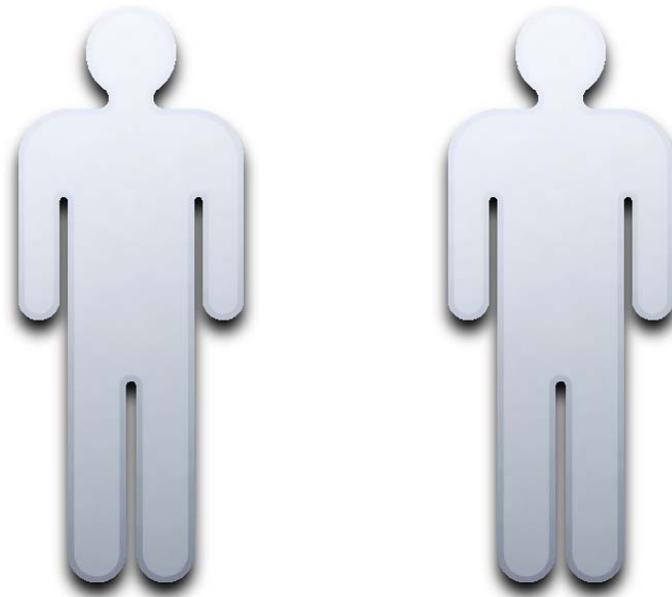
# Response to Violations

---

- **All observations of a Two-Person Rule violation must be immediately reported to supervision/line management and to the MBA Custodian.**
- **The MBA Custodian is responsible for reporting the violation to site Material Control and Accounting.**
- **Appropriate actions must be taken to verify that all accountable nuclear materials are present.**

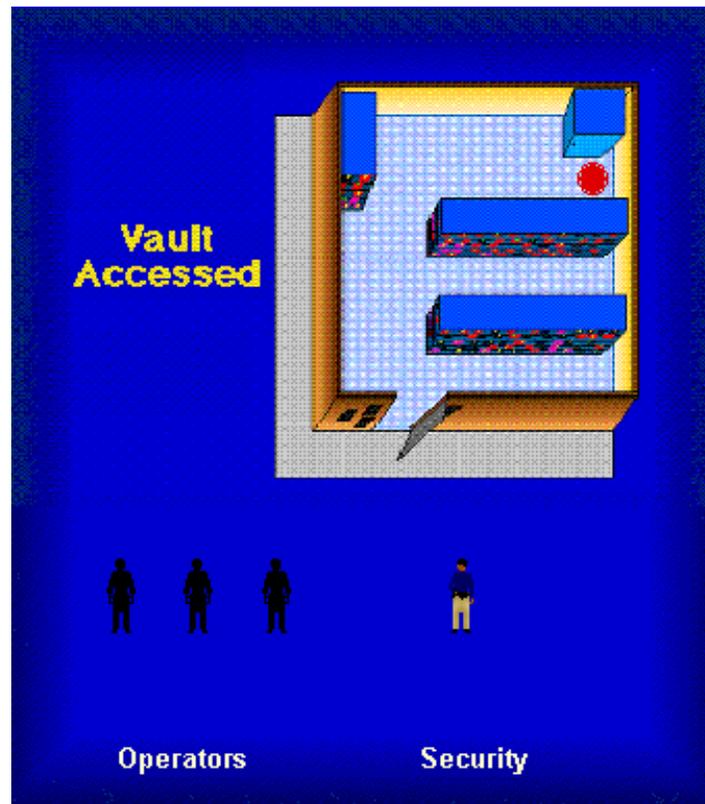
# Two-Person Rule Scenarios

---



# Two-Person Rule Scenario 1

- The storage area of Category I SNM is in access mode for inspection of shipping containers and the work to be performed is at the red dot.



November 2008

Lecture 4 -48

Lecture 3 Targets - 48

# Two-Person Rule Scenario 1

- The storage area of Category I SNM has been accessed for inspection of shipping containers and the work to be performed is at the red dot.



*\*Incorrect: The door is not observable by the team*

November 2008

Lecture 4 -49

Lecture 3 Targets - 49

# Two-Person Rule Scenario 1

- The storage area of Category I SNM has been accessed for inspection of shipping containers and the work to be performed is at the red dot.



*\*CORRECT!*

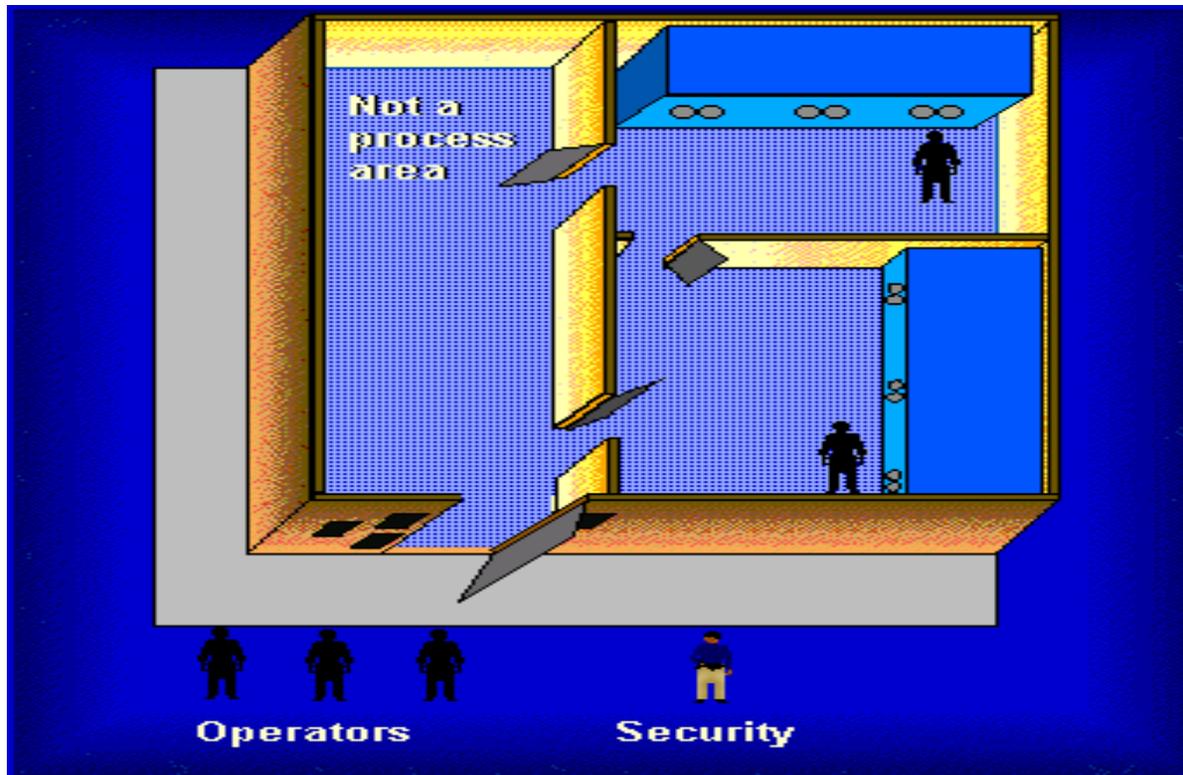
November 2008

Lecture 4 -50

Lecture 3 Targets - 50

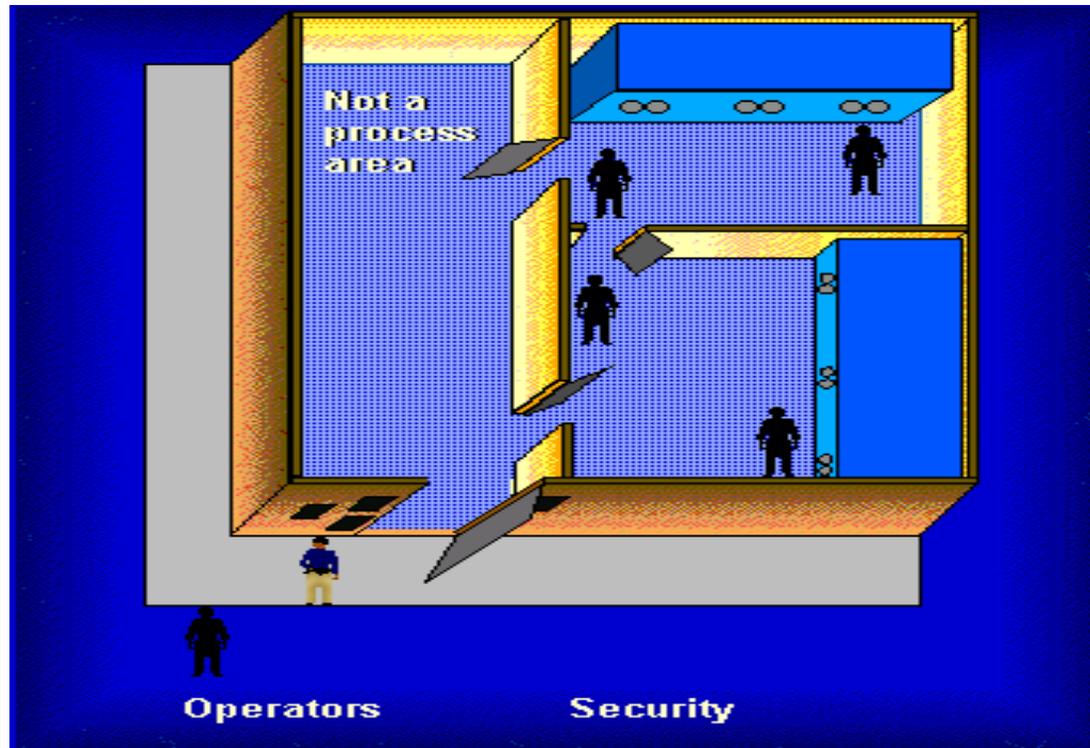
# Two-Person Rule Scenario 2

- Work is to be performed in the glove box area to produce nuclear material products.



# Two-Person Rule Scenario 2

- Work is to be performed in the glove box area to produce nuclear products



*\*CORRECT!*

November 2008

Lecture 4 -52

Lecture 3 Targets - 52



# Lecture 4.1

---

## Two Person Rule



# Learning Objective

---

- **Understanding the purpose of the two person rule**
- **Understanding how and where the two person rule is implemented**

# Purpose of the Two-Person Rule

---

- **The primary purpose of the Two-Person Rule is to ensure that no single individual is in a position to divert, remove, or sabotage special nuclear material without timely detection.**
- **This single individual or insider threat can be any person currently working within your facility or a person not directly related to day-to-day operations.**

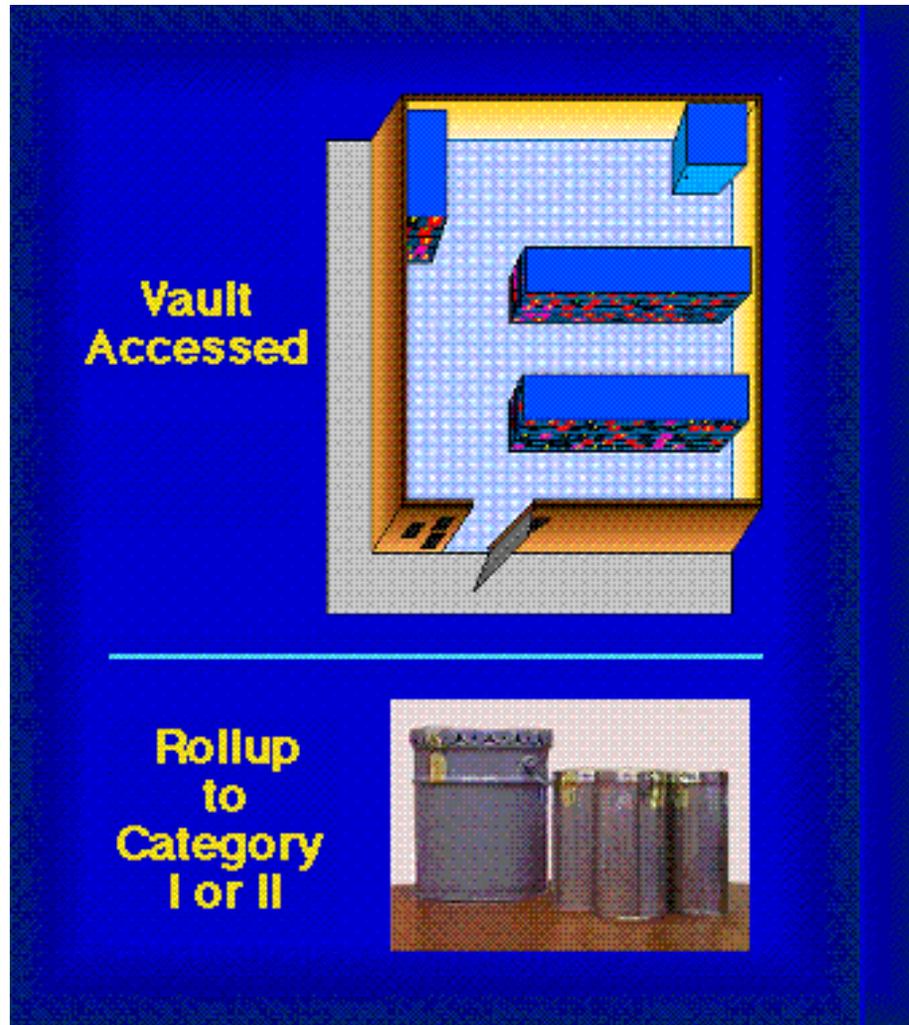
# **When to Apply the Two-Person Rule**

**The Two-Person Rule must be used when personnel have access to quantities of SNM and:**

- the material is NOT protected by an active security alarm system or other material surveillance mechanisms.**
- smaller quantities of material can be easily accumulated into a Category I or II quantity.**

# Examples

---



November 2008

Lecture 4.1 -5

# When to Apply the Two-Person Rule

(cont'd)

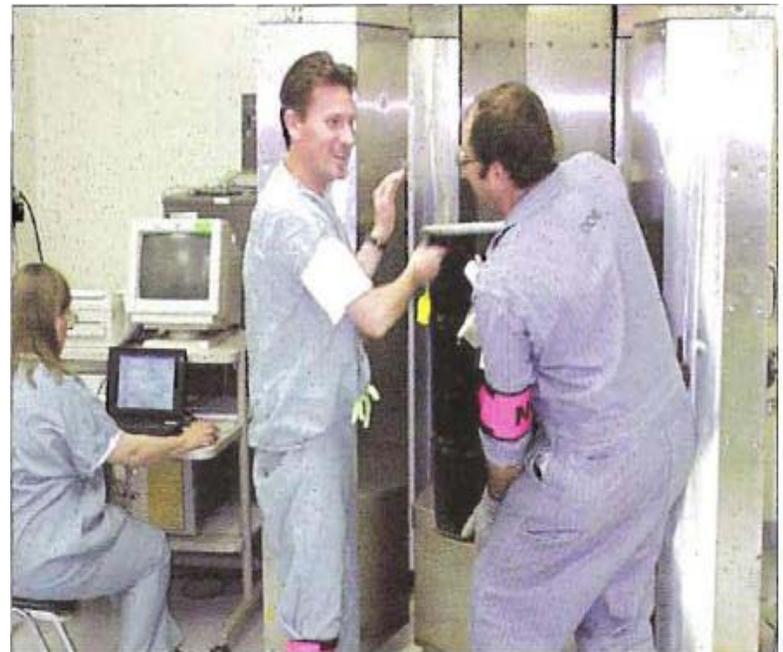
---

- **The application of the Two-Person Rule can be associated with a wide assortment of conditions in the facility. These conditions can include SNM production, packaging, measurements, material transfers, and SNM not under secured storage conditions.**
- **Routine facility maintenance of general access into areas where these quantities of SNM are located would also require the application of the Two-Person Rule.**

# Principles to Follow

There are three basic principles that must be followed at all times when participating as part of a Two-Person Rule team:

- Clearly observe each other at all times
- Observe the special nuclear material or access to that material
- When accessed, at least one member of the Two-Person Rule team must observe the entrance to storage areas



## **Principles to Follow** (cont'd)

---

- **If any work in the facility where a Two-Person Rule is required cannot meet these requirements, work must be stopped and unobservable workers must exit the area.**
- **All outside visitors must be observed by a Two-Person Rule team. Depending on the size of the group, this task may require more than two people.**
- **Documentation of the Two-Person Rule participants is required when used. Procedures or log sheets may be used to document compliance with the Two-Person Rule.**

# Requirements for a Two-Person Rule Participants

Each person must meet all of the following requirements before they can be part of a Two-Person Rule Team:

- Properly cleared for the category and amount of special nuclear material being controlled
- Knowledgeable of correct facility procedures
- Authorized to be part of the Two-Person Rule
- Complete the required Two-Person Rule training



# Locations for Two-Person Rule Application

---

There are certain areas where the Two-Person Rule must be applied. These areas include:

- **Secure storage areas**
- **Process lines with Category I or II quantities of SNM**
- **Areas with high sabotage potential**
- **Safeguards and security systems**
- **Material transfers across MAA boundaries of Category I and II SNM items**

# Locations for Two-Person Rule Application (cont'd)

## Secure Storage Areas

- **Secure storage areas include storage areas used for the storage of Category I and II quantities of SNM. There are several Two-Person Rule requirements that must be followed for these areas.**



# Locations for Two-Person Rule

## Application (cont'd)

### Secure Storage Areas (cont'd)

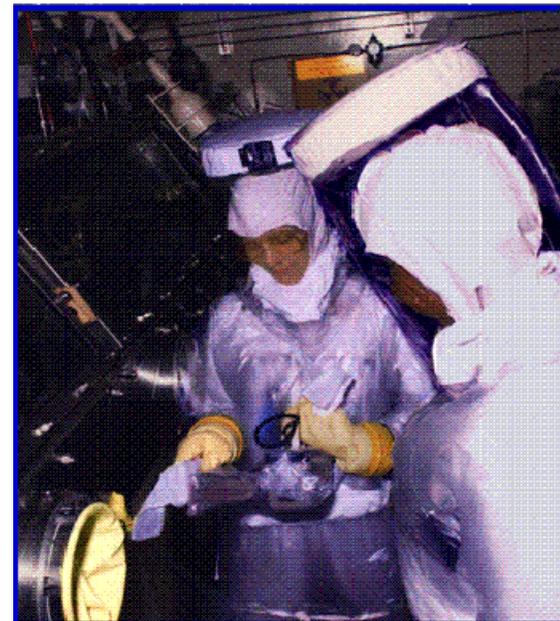
---

- **Upon Entry into a secured storage area, personnel must:**
  - **Have access authorization checked**
  - **A minimum of two authorized persons are required to enter storage area**
  - **Be capable of clearly observing each other at all times**
  - **Be capable of observing SNM or access to SNM**
  - **Have constant observation of entrance (by at least 1 team member)**
  - **Additional persons may need to be added to the two-person rule surveillance team in order to accomplish all of the above tasks and complete the assigned work in the storage area.**

# Locations for Two-Person Rule Application (cont'd)

## Process Line

- **Process lines or production areas that have Category I and II quantities of SNM and are accessible by personnel in the work area require the application of the Two-Person Rule.**
- **These manufacturing areas can include chemical/mechanical processing lines, glove boxes, maintenance aisles, huts, repackaging areas, and assay areas.**



# Locations for Two-Person Rule Application (cont'd)

## Process Line (cont'd)

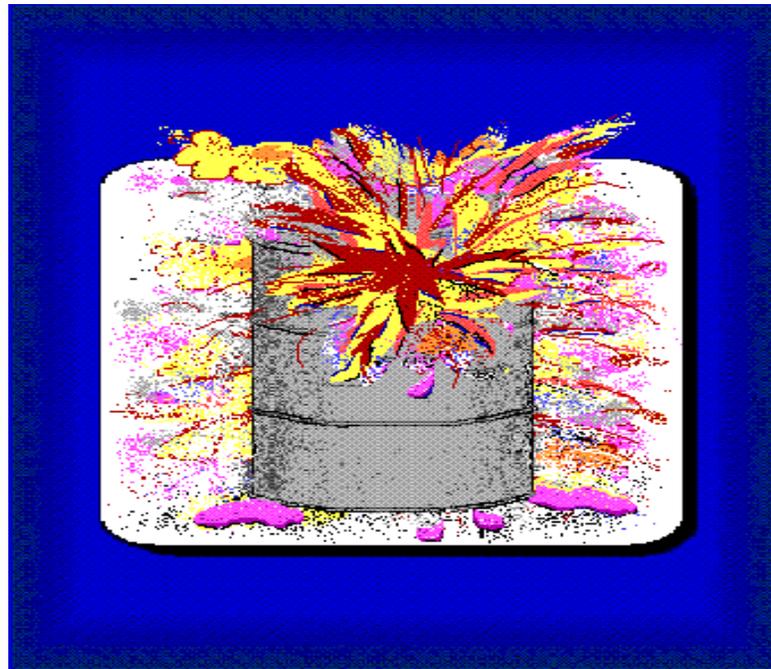
---

- **Since process area entries are in a storage area, watching those entries is NOT required. However, it is the responsibility of the persons entering the area to comply with the Two-Person Rule requirements upon entry.**
- **One person can be assigned to watch several other workers as long as all Two-Person Rule requirements are met.**

# Locations for Two-Person Rule Application (cont'd)

## Sabotage Potential

- A Two-Person Rule is required in all areas where sabotage risks are designated as “High”.
- All personnel must be alert for the potential sabotage of SNM and the production of SNM.



# Locations for Two-Person Rule Application (cont'd)

## Safeguards and Security Systems

- **Key safeguards and security systems can include portal monitors, classified computer systems, and access control systems where SNM is located. Required maintenance on these systems must be performed by a two-person team. Both members must be knowledgeable of work being performed on the safeguards and security system.**



# Locations for Two-Person Rule Application (cont'd)

## Material Transfers Across Material Access Area Boundary

---

- **A Two-Person Rule is required to transfer all radioactive materials out of a Material Access Area (MAA). Radioactive material includes all accountable nuclear material (e.g., HP sources, technical standards, process samples). These types of items can set off a portal monitor alarm upon being checked at the MAA boundary.**

# Locations for Two-Person Rule

## Application (cont'd)

### Material Transfers Across Material Access Area Boundary (cont'd)

---

- Any person who signs to authorize a nuclear material transfer cannot be part of the Two-Person Rule team carrying the material out of the MAA.
- Transfer documentation and authorization prior to releasing the material for MAA are required.
- The protective force at the MAA boundary checks for adherence of the Two-Person Rule requirement for transferring radioactive material out of the MAA.

# Tamper Indicating Program

---

- **A device that may be used on items such as containers and doors, which because of its uniqueness in design or structure reveals violations of container integrity.**
- **Or Simply - Devices that indicate, upon proper inspection, whether tampering or entry has occurred.**

# Tamper Indicating Program

---

- **The use of two authorized TID Applicators protects against a single person diverting or substituting material being placed in a storage or shipping container. Both persons are responsible for ensuring that the correct material is placed in the container prior to the application of the TID seal. Both persons are also responsible for ensuring the seal is applied correctly and is intact (integrity).**

# Tamper Indicating Program (cont'd)

---

- The application, removal, and destruction of TIDs require the use of two authorized TID Applicators.



# Nuclear Material Physical Inventories

---

- A Two Person inventory team is used to ensure the validity of information collected during a physical inventory.



# Nuclear Material Physical Inventories

(cont'd)

---

- **Physical inventories are taken for each material balance area (MBA) in order to obtain an accurate accounting of the nuclear material that is present in the facility.**
- **Two-person inventory teams systematically search through the entire facility to physically locate all nuclear material.**

# Other Uses of Two Person Teams

---

- There are other activities which require the use of two person teams, where it is not necessary for those persons to be Two-Person Rule qualified. For instance, TID application and inventories for any Category of material or any reason require two person teams.

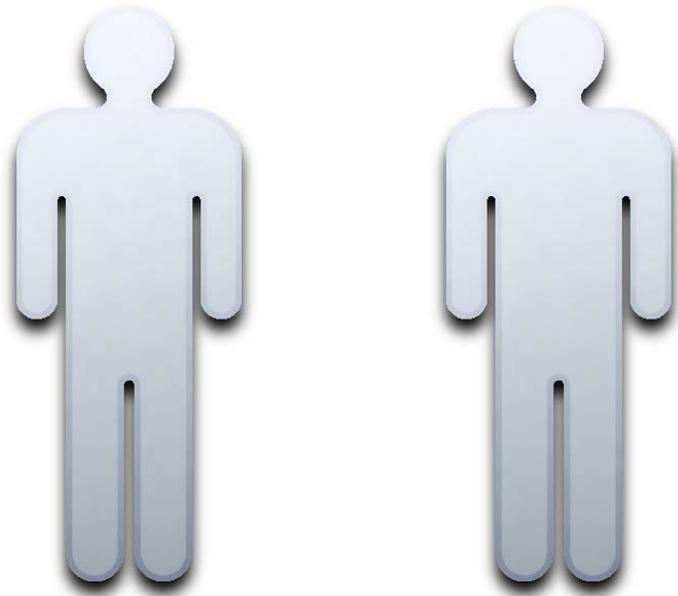
# Response to Violations

---

- **All observations of a Two-Person Rule violation must be immediately reported to supervision/line management and to the MBA Custodian.**
- **The MBA Custodian is responsible for reporting the violation to site Material Control and Accounting.**
- **Appropriate actions must be taken to verify that all accountable nuclear materials are present.**

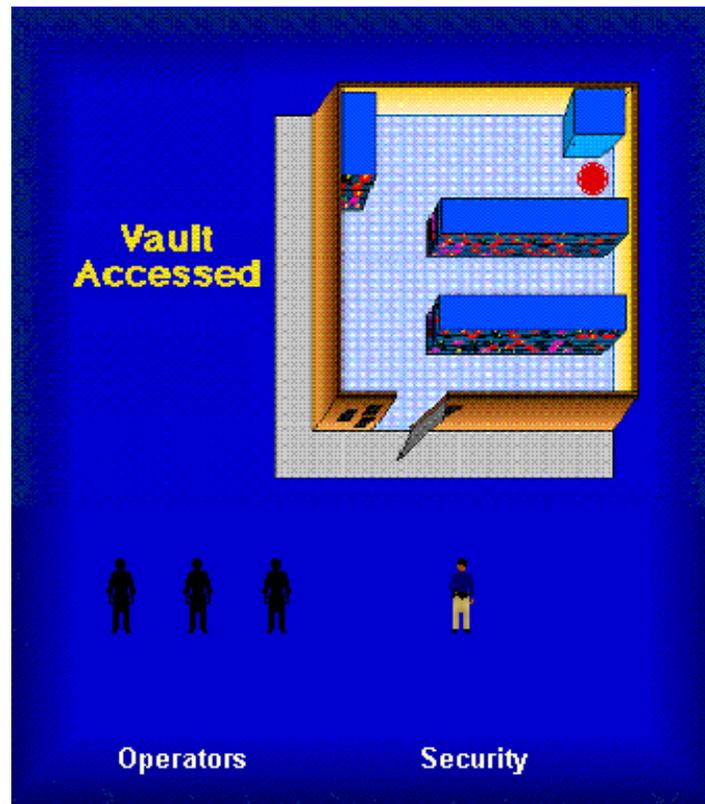
# Two-Person Rule Scenarios

---



# Two-Person Rule Scenario 1

- The storage area of Category I SNM is in access mode for inspection of shipping containers and the work to be performed is at the red dot.



# Two-Person Rule Scenario 1

- The storage area of Category I SNM has been accessed for inspection of shipping containers and the work to be performed is at the red dot.



*\*Incorrect: The door is not observable by the team*

# Two-Person Rule Scenario 1

- The storage area of Category I SNM has been accessed for inspection of shipping containers and the work to be performed is at the red dot.



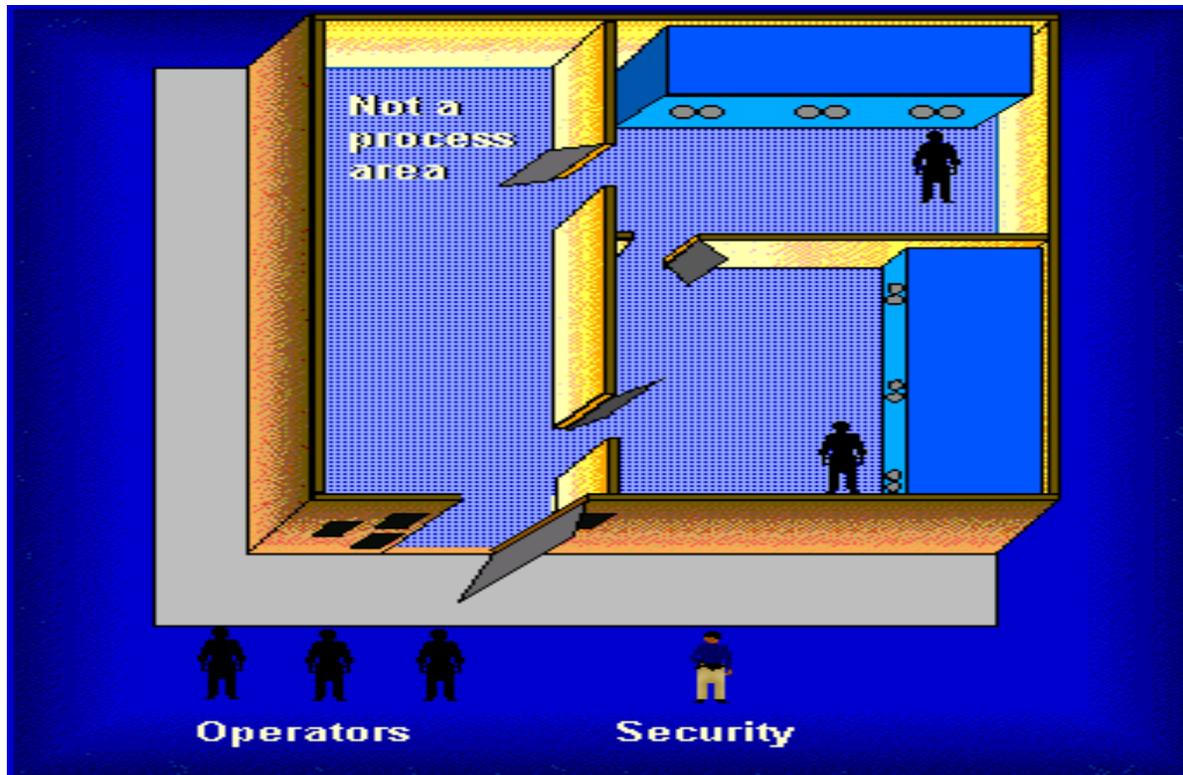
*\*CORRECT!*

November 2008

Lecture 4.1 -29

# Two-Person Rule Scenario 2

- Work is to be performed in the glove box area to produce nuclear material products.



# Two-Person Rule Scenario 2

- Work is to be performed in the glove box area to produce nuclear products



*\*CORRECT!*

November 2008

Lecture 4.1 -31



# Lecture 5

---

## Technical Measures



Lawrence Livermore  
National Laboratory



# Learning Objective

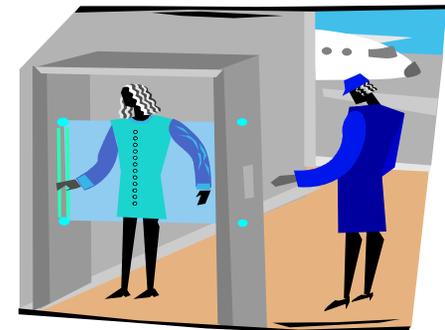
---

- **Review Insider Protection System Approach**
- **Identify technical measures of an MPC&A system that can provide protection against insider threats**
- **Estimate the effectiveness of technical measures**

# Technical Measures

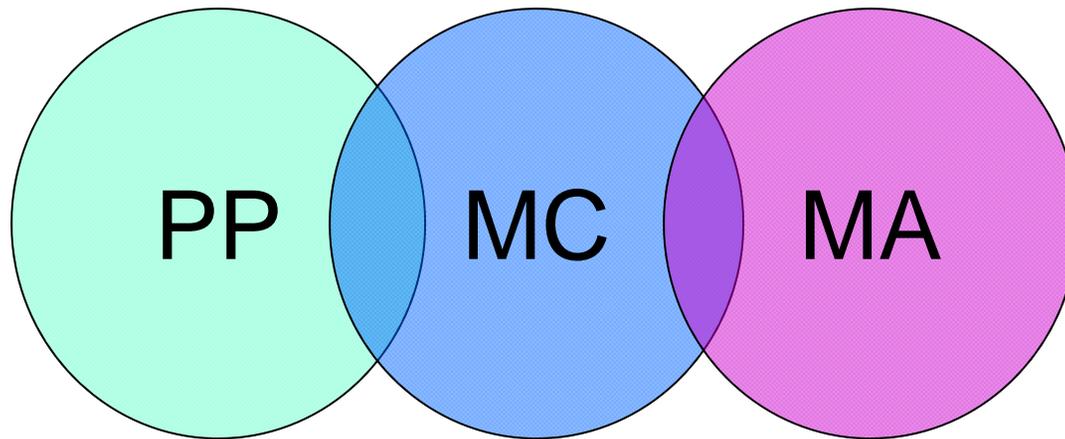
---

- **Physical Protection**
- **Material Control and Accountability (MC&A) programs**
- **Operational**



# Safeguards Integration

---



**All disciplines, Physical Protection (PP), Material Control (MC), and Material Accounting (MA), working together are critical to effective insider mitigation.**

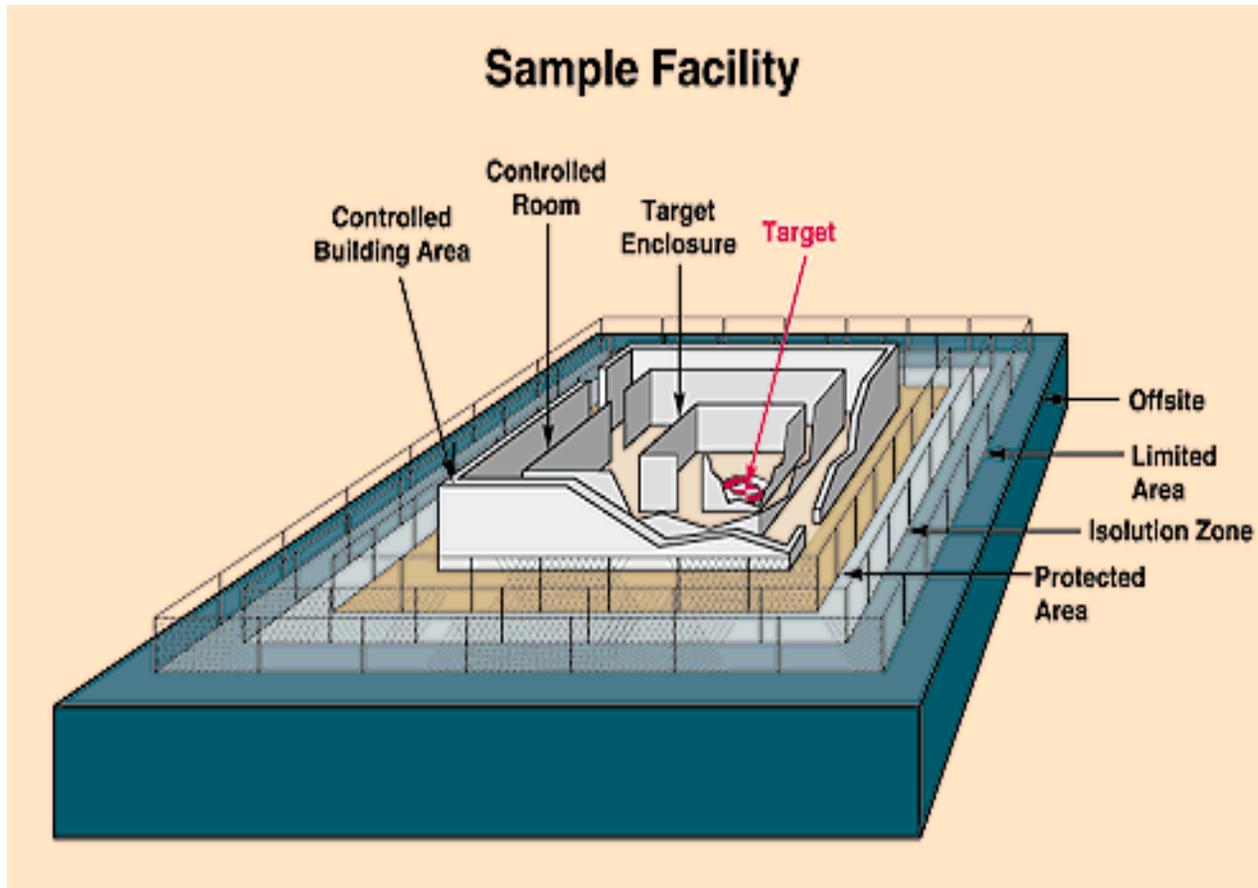
# Nuclear Facility Design

---

- Facility design can minimize opportunities for theft and sabotage
- Security is established in concentric rings or layers
- Protection in Depth
  - Multiple layers must be traversed upon entry or exit
- Balanced protection
  - Protection elements on a given layer provide equal protection
    - Weakest link generally exploited
- Hardened critical systems
  - Tamper resistance
  - Cyber protection
- Process design and/or the way the process is operated can minimize physical inventory uncertainty (LEID)
- Barrier and delay systems slow activity of insider

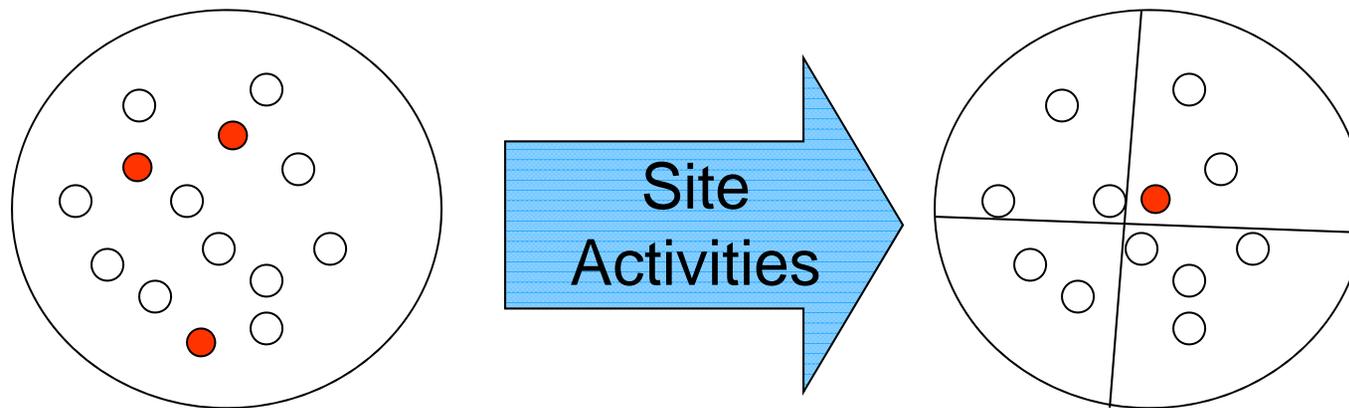


# Layered Protection



# Further Reduce Potential Adversaries

- **Compartmented activities further reduce potential insiders**



- - persons with desirable behavior
- - persons with undesirable behavior

# Manned Portal Monitoring

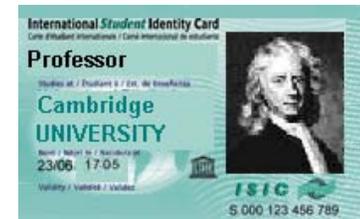
- **Monitoring of material being moved through boundary (PA, MAA, and MBA)**
- **All Personnel and vehicle entering or leaving the MAA or PA are subject to monitoring**
- **Metal detectors used to detect shielding**
- **Insiders trying to remove SNM**

**Effectiveness of this safeguard element is critically tied to MC&A Material Transfer Procedures, Measurement, and Material Control Procedures.**



# Physical Protection Entry/Exit Control

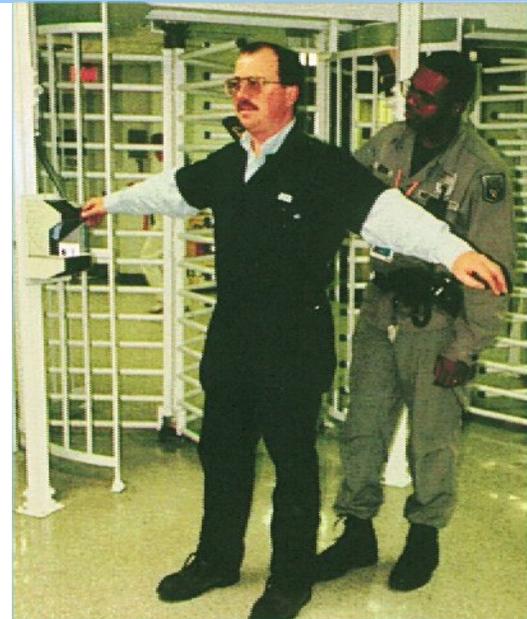
- **Authorization using:**
  - **Picture badge inspection**
  - **Electronic credential**
  - **Personal identification number (PIN)**
  - **Badge exchange**
  - **Biometrics**



# Physical Protection

## Entry/Exit Control *(cont'd)*

- **Contraband detection**
  - **Metal detector**
  - **Explosives detector**
  - **X-ray for packages**
  - **Nuclear material detector**
    - **Medical isotopes**
  - **Package inspection by personnel**
  - **Personnel search**
    - **Routine and random**
- **Emergency exit controls and proc**



# Physical Protection Entry/Exit Control *(cont'd)*

---

- Personnel restriction after emergency exit
- Emergency exit controls and procedures



# Metal Detectors

---

- **Entry**
  - Adjusted to detect weapons
- **Exit**
  - Adjusted to detect shielding material
- **General**
  - Operational testing
  - Sensitivity testing and calibration
  - Personnel training



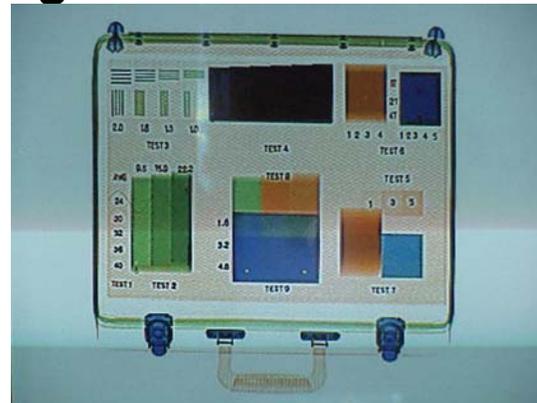
# Trace Explosives Detectors

- **Entry**
  - Detects either macroscopic amounts of material or minute amounts of vapor or particles
  - Must consider likely nuisance alarm sources
- **General**
  - Operational testing
  - Sensitivity testing and calibration
  - Personnel training
  - Can use either electronic or animal detectors



# X-ray Package Inspections

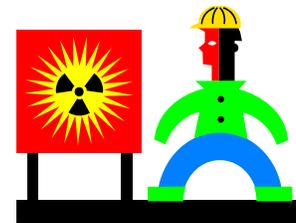
- **General**
  - Calibration is needed – use a step wedge or suitable approved test kit
  - Personnel training is critical to success
- **Entry**
  - Inspect packages for weapons and explosives
- **Exit**
  - Inspect packages for shielding or nuclear material



# Nuclear Radiation Monitors

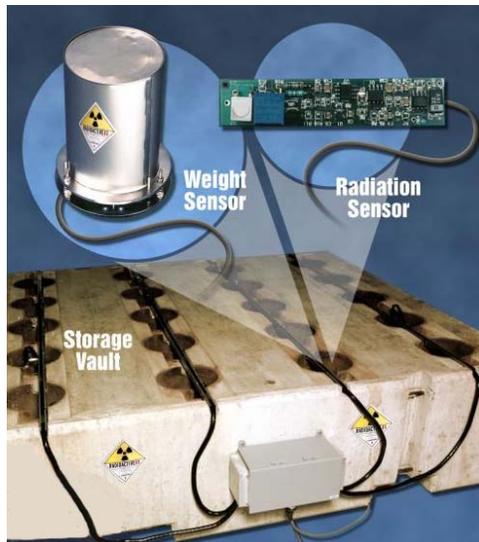
---

- **Entry**
  - To prevent those persons from entering who will cause alarms when they leave the facility because of medical isotopes or off-site contamination
- **Exit (two types)**
  - NM - to detect nuclear material leaving the facility
  - Safety - to detect contamination
- **General**
  - Operational testing
  - Sensitivity testing and calibration



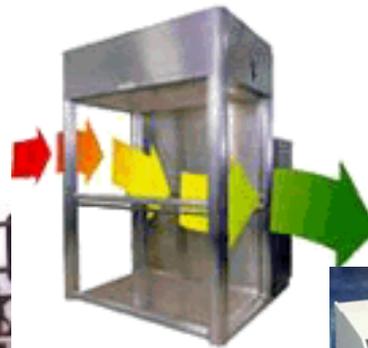
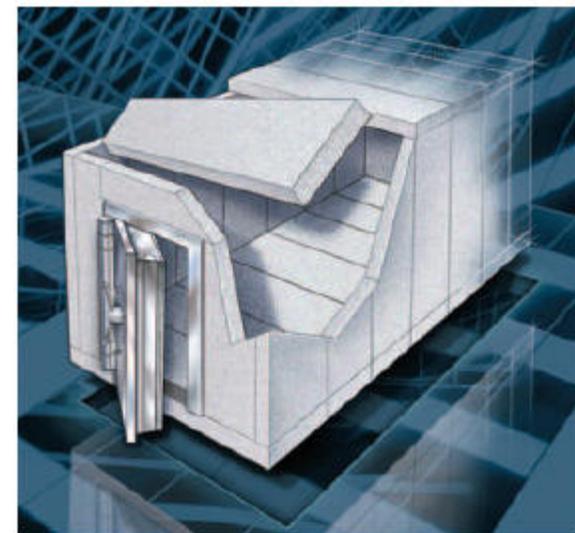
# Surveillance Systems

- Video
- Intrusion systems (volumetric, infrared, vibration)
- Door alarms
- Microwave....



# Barriers and Delay systems

- Fences
- Hardened walls and doors
- Locking mechanisms (e.g., combinations, multiple, electronic)



November 2008

Lecture 5 -17

# Nuclear Material Control and Accountability (MC&A) Program

---

## Materials Accountability

- Tracks material quantities and locations
- Provides loss detection/assessments



## Materials Control

- Governs material movement, location and use
- Detects and assesses unauthorized activities

## Measurement Program

- Manages instrumentation/equipment used to establish nuclear values

# Materials Accounting Technical Measures

---

- **Accounting systems**
- **Statistical/engineering techniques used to establish and evaluate the inventory and inventory differences (e.g., LEID models, process monitoring)**
- **Vault or storage position monitoring systems (e.g., continuous monitoring of items in storage)**



# Materials Control

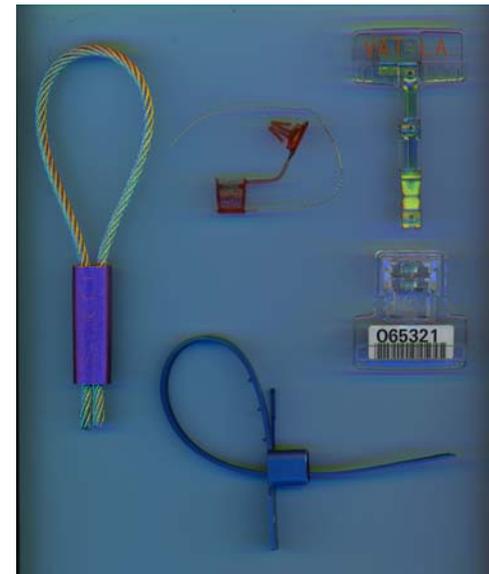
## Technical Measures

---

- **Material containment working with PP systems relative to Limited Area (LA), Protected Areas (PA), Material Access Areas (MAA), and Storage Areas procedural controls**
- **Tamper Indicating Devices (e.g., TIDs or Seals) both passive and active**
- **Materials surveillance again working with PP systems to control and monitor access to materials**
- **Physical barriers (e.g., doors, restraints on storage locations, etc.)**

# Tamper Indicating Devices

- Detect attempts to access material or locations
- Provides no physical protection
- Used in combination with other systems
- TIDs applied:
  - After measurements
  - After inventories
  - During transportation



# Material Tie-Downs

**Material tie-downs can be used to add delay.**

**They can be used to control access and hence unauthorized removal of nuclear materials.**

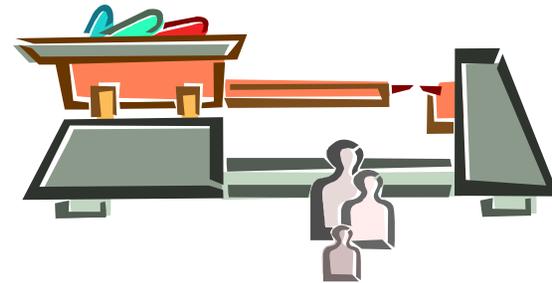


# Measurement Program

## Technical Measures

---

- **Provides quality assurance and control for the measurement processes**
- **Ensures measurement methods are proper for the material being measured and the values being produced are correct**
- **Ensures measurement systems are working correctly (e.g., performing to their design requirements)**



# Material Transfer Procedures

---

- **Verification of receivers authorization and need to receive the material**
  - **Detects attempts to ship material to a bogus receiver**
- **Material measurements**
  - **Detects diversions of material during the transfer process**
- **Transfer checks**
  - **Provides rapid detection of gross anomalies**
- **Documentation transferred through separate channels**
  - **Detect falsification of data as a possible way to hide theft**

# Shipping Monitors

---

- **Shipping portals**
- **Vehicle Truck Portals**
- **Waste (clean and contaminated)**

# Waste Monitoring

---

- **Detect theft or diversion through waste streams**
- **Identify all waste streams that cross boundaries (PA, MAA, MBA)**
- **Physical inventories and evaluation of inventory adjustments are part of a overall program**
- **Installing, maintaining, and monitoring waste monitoring equipment**

# Operational Process Alarms

## Technical Measures

---

- **Processing and engineering controls to monitor operational process**
- **Safety alarms for abnormal conditions (e.g., fire, criticality, contamination, glove box airflow, etc.)**
- **Measurement equipment to monitor process parameters** (*note: measurement equipment sometimes dual use with MC&A*)



# Summary of Technical Protection Measures

---

- **Facility Design**
- **Physical Protection**
  - **Access Controls**
  - **Barriers**
  - **Surveillance Systems**
- **Material Control and Accounting**
- **Operational alarms**





# Lecture 6

---

## Detection, Assessment Recovery, and Prosecution



# Learning Objective

---

- **Identify MPC&A Detection Elements**
- **Identify MPC&A Assessment Elements**
- **Video Exercise**

# Definitions

---

- **Detection element:** any component of a facility's MPC&A system which can generate an alarm indicating an abnormal condition or event involving the control, or possible loss of SNM
- **Assessment Element:**

# MC&A Contribution to Anomaly Detection

---

- **Detection of anomalous activities are frequently divided into two categories:**
  - **Prompt – during the adversary action, and**
  - **Delayed – after the adversary action has been completed or is in progress**
- **MC&A contributes to both prompt and delayed detection**

**Complete evaluation of MPC&A system effectiveness requires consideration of the integrated system of BOTH MC&A and Physical Protection elements**

# Prompt Detection

---

**Prompt detection applies primarily to abrupt theft scenarios or “single events” related to protracted theft scenarios**

- **Protracted scenarios: multiple thefts of smaller quantities of nuclear material to accumulate the desired quantity**
- **Multiple thefts increase the probability of detection before the desired quantity is accumulated**
- **Smaller quantities make detection of individual thefts more difficult**

# Examples of Prompt Detection

---

- **Observation by co-workers or supervisors - two person rule detect unauthorized removal from glove box**
- **Technical measures**
  - **Access control – metal detector detects removal of shielded SNM**
  - **Signal line tamper detection**
  - **Operational alarm – detects high pressure in glove box**
  - **Item monitoring**



# Delayed MC&A Detection Elements

---

- **Physical inventories and measurements**
- **Internal and external transfer procedures**
- **Material control indicators: shipper/receiver differences, inventory differences, normal operating losses**
- **Trend analysis of material control indicators and process data**
- **Statistical analysis of measurement and measurement control data**
- **Daily administrative checks**

# Material Transfer Procedures

---

- **Verification of receivers authorization and need to receive the material**
  - **Detects attempts to ship material to a bogus receiver**
- **Material measurements**
  - **Detects diversions of material during the transfer process**
- **Transfer checks**
  - **Provides rapid detection of gross anomalies**
- **Documentation transferred through separate channels**
  - **Detect falsification of data as a possible way to hide theft**

# Review of Accounting Adjustments

---

- **Detects inappropriate or inconsistent adjustments that may be indicators of anomalies**
- **Personnel reviewing the reports must be knowledgeable of the process and what is “normal”**

# Quality Verification

---

- **Verification of the accuracy of the data entered into the accountability records**
  - **Detects mistakes and false data**
- **Verification of operational activities**
  - **Detects unauthorized activities through personal observation**

# Signal Line Tamper Detection

---

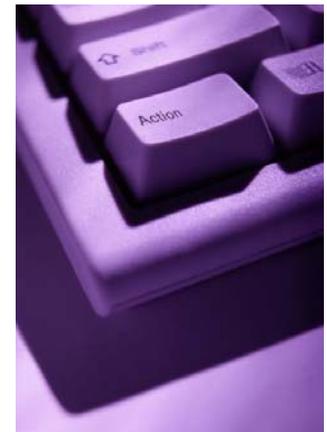
- **Provides assurance that the data on protection system signal lines has not been tampered with**
- **Protects against an insider compromising either the data or the signal path as part of a malevolent act**
- **A multi-person maintenance rule, knowledgeable escort, or detailed testing after maintenance is needed to assure desired capability is not compromised**
- **Periodic testing**



# Assessment At Site: Two Steps

---

- 1. The immediate assessment action to prevent the malevolent action from occurring – security personnel, operations personnel**
- 2. Immediate operational action taken by the system and operating personnel to prevent the malevolent act from resulting in the material theft**
  - **Safety and emergency personnel (applies to sabotage)**



# Immediate Personnel Assessment

---

- **Detection by coworkers or security system might have occurred during procedure violation, unusual activity, etc.**
- **First assessment might be by the person detecting the activity (co-worker) – part of security awareness training:**
  - **Security should be immediately notified and rapidly confront both the violent and non-violent adversary**
  - **Could include challenging the adversary to delay or stop his action**
  - **Notify manager**

# Operational Process Assessment

---

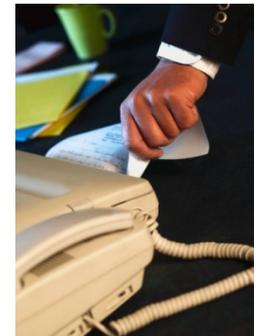
- **Operations immediately negate the undesirable consequence**
- **Follow safety and security emergency response plans under a technical crisis team**
- **Identify anomalies**
- **Return system to protected state**
  - **Repair damage**
  - **Replace parts**
  - **Compensate for security weaknesses**



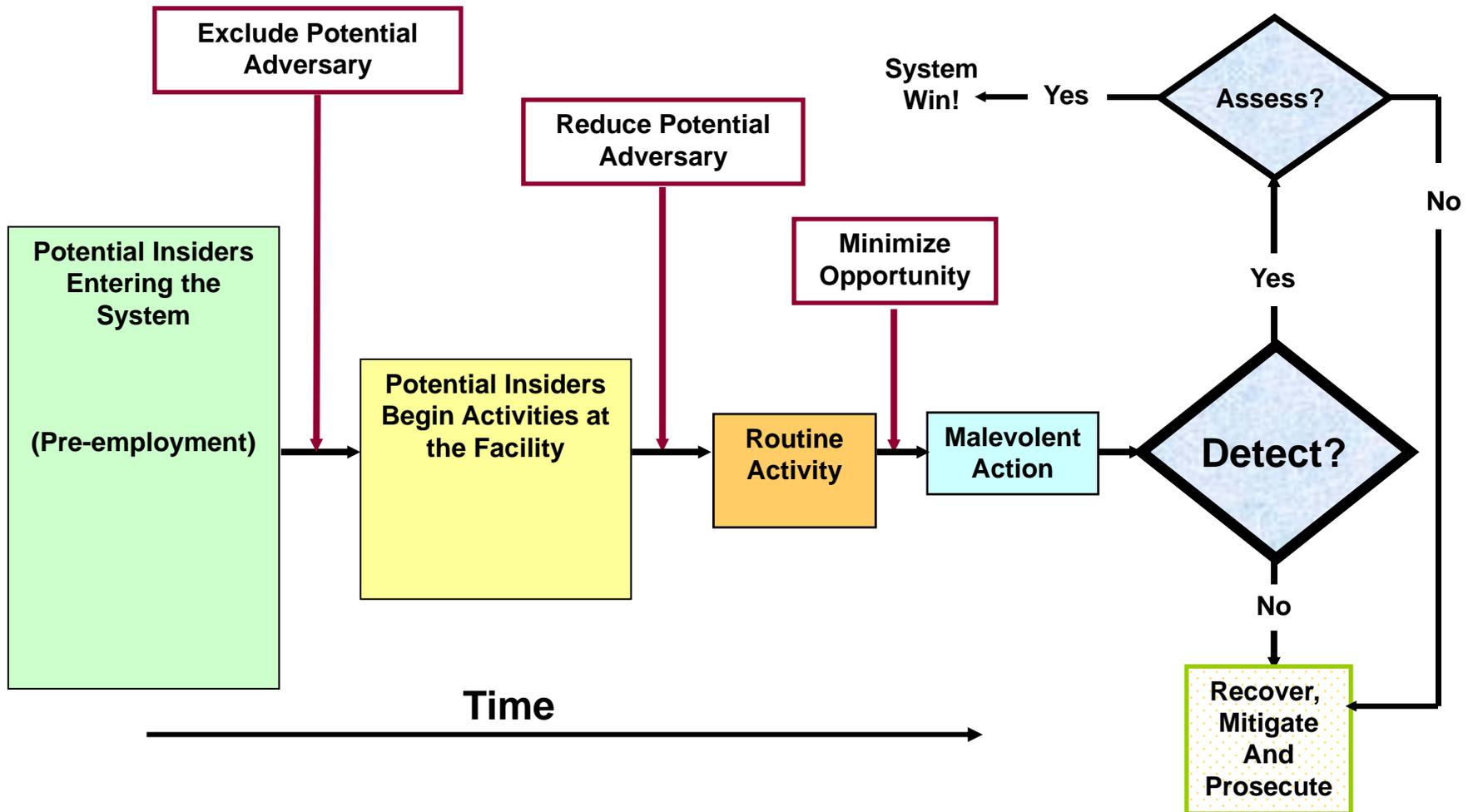
# Compromise of Information

---

- Often not detected in a timely manner
- Coworkers could detect compromise such as unauthorized faxing, copying, conversation, E-mail, activities, etc.
- Reporting could be by the person detecting the activity
  - Part of security awareness training
- Security organization should be notified
- Incident program
- Investigation of perpetrator and information passed should begin immediately



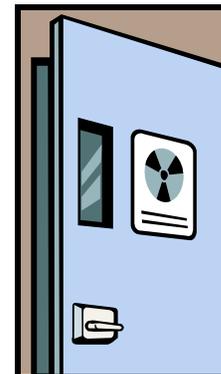
# Insider Protection System Approach



# Malevolent Actions - Examples

---

- **Removing material**
  - **Abrupt**
  - **Protracted**
- **Defeating or attempting to defeat the MC&A system**
- **Bypassing or compromising plant safety or security measures**
- **Defeating or attempting to defeat the operational process monitoring**
- **Damaging or compromising equipment**
- **Attacking or influencing personnel**
- **Falsifying records**
- **Others?**



# Detection Of Malevolent Actions - Issues

---

- **Insider tries to hide his actions or make them look normal**
  - **Uses deceit and stealth much more than force**
- **Detecting actions**
  - **Includes administrative, technical, and procedural measures**
- **A continuous timeline may be relevant in some cases and not in others (protracted vs. abrupt)**
- **Detection may be a function of time and/or the number of events**
- **Analysis and investigation can result in detection**

# Detection Of Malevolent Actions - Issues *(cont'd)*

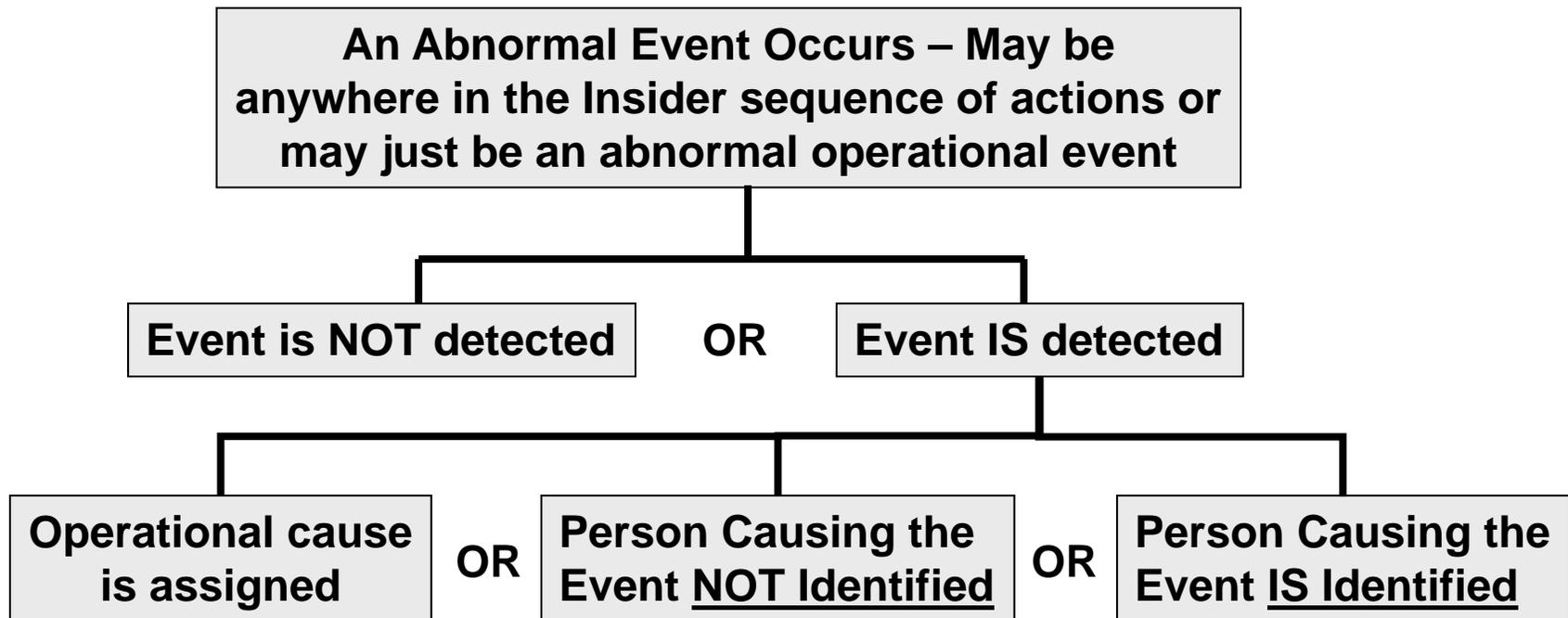
---

- **Detection for insiders can only be possible when they do something abnormal or malevolent**
  - Acquire target
  - Change records
- **Assessment to confirm malevolence may be difficult**
  - Assumption of innocence
  - Hesitation to report co-worker
  - Fear of questioning authority
- **Insider may test detection and assessment systems to assess their effectiveness**
- **Coworker may be hesitant to report suspicious behavior**

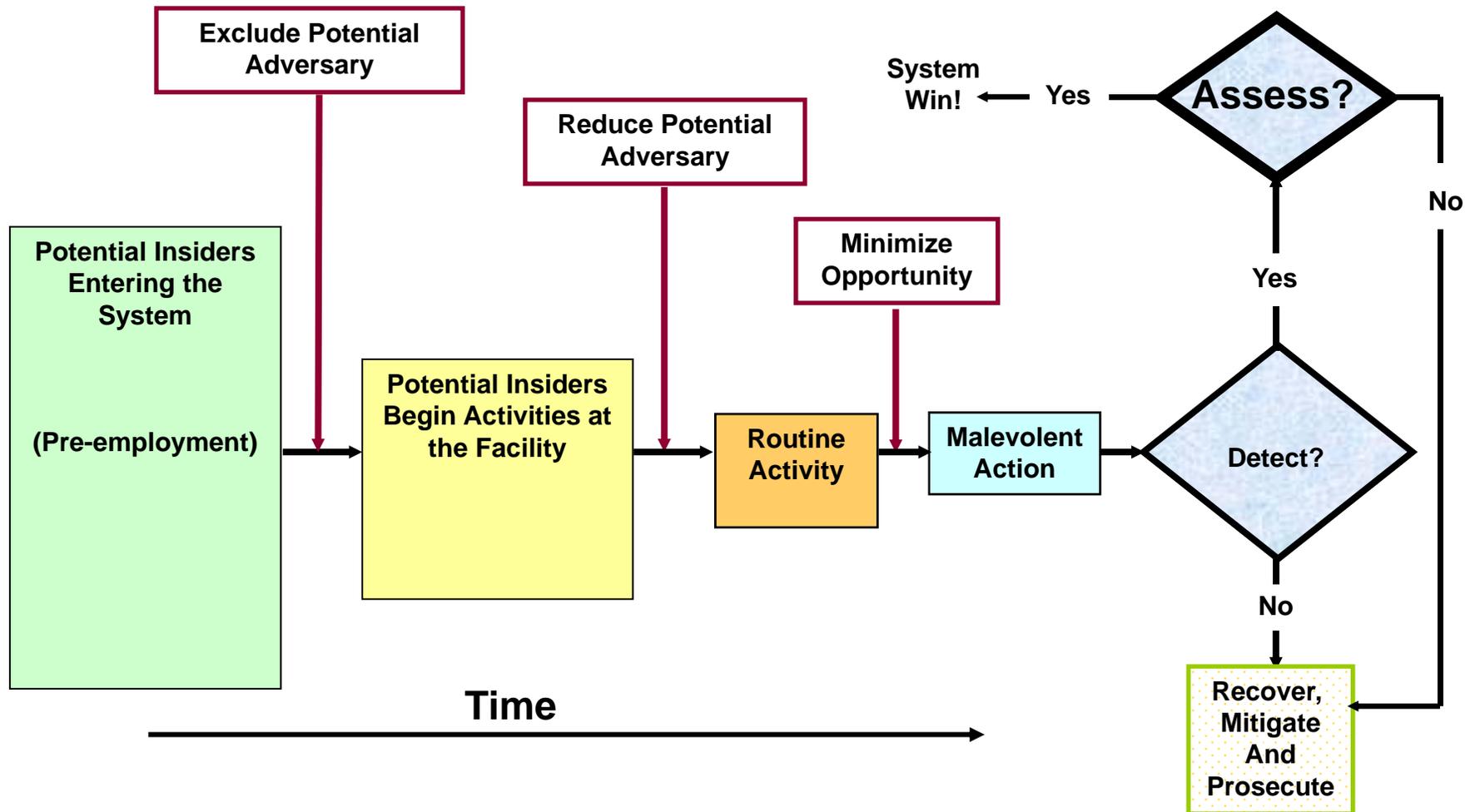


# Detection Considerations

---



# Insider Protection System Approach



# Assessment Elements

---

- **Protective force assesses**
  - **Metal detector alarm – hand search**
  - **SNM detector alarm**
  - **Other alarms**
- **Two person rule (knowledgeable second worker) provides assessment**
- **Surveillance systems**
- **Administrative checks**
- **Transfer verification**
- **Inventory difference resolution**
  - **Additional inventories**
  - **Additional process measurements**

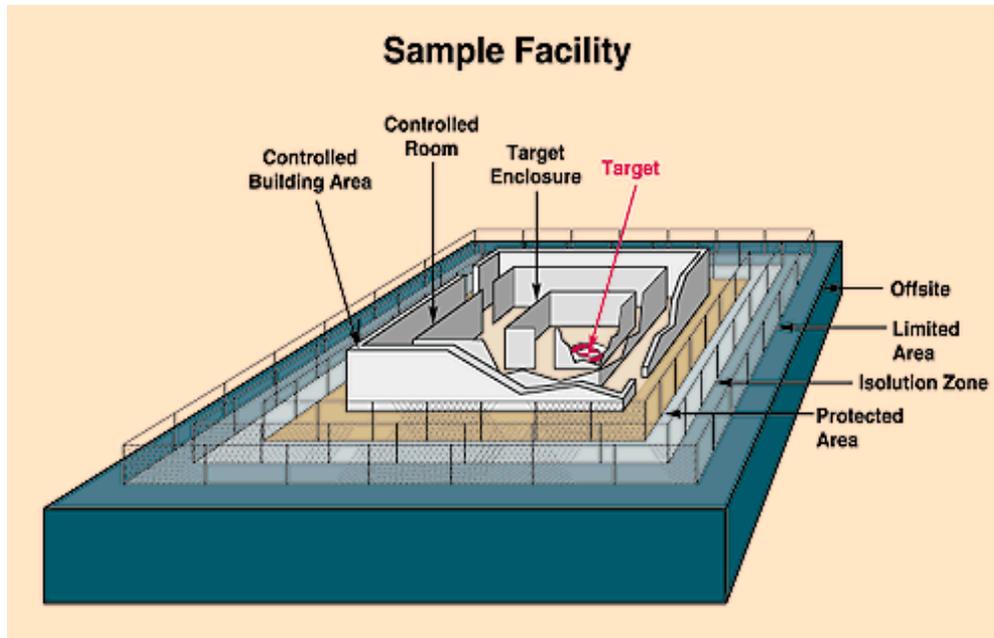
# Immediate Personnel Assessment to Prevent Malevolent Action

---

- **Assessment may vary depending on the type of adversary**
  - **Covert insider**
  - **Overt insider(s)**
- **Assessment will also vary depending on**
  - **How detection occurs**
    - **Protective force**
    - **Co-workers**
    - **Operational / safety system**
  - **What is detected**
    - **Obvious malevolence**
    - **Operational procedure error**



# Protective Force Role in Insider Detection & Assessment

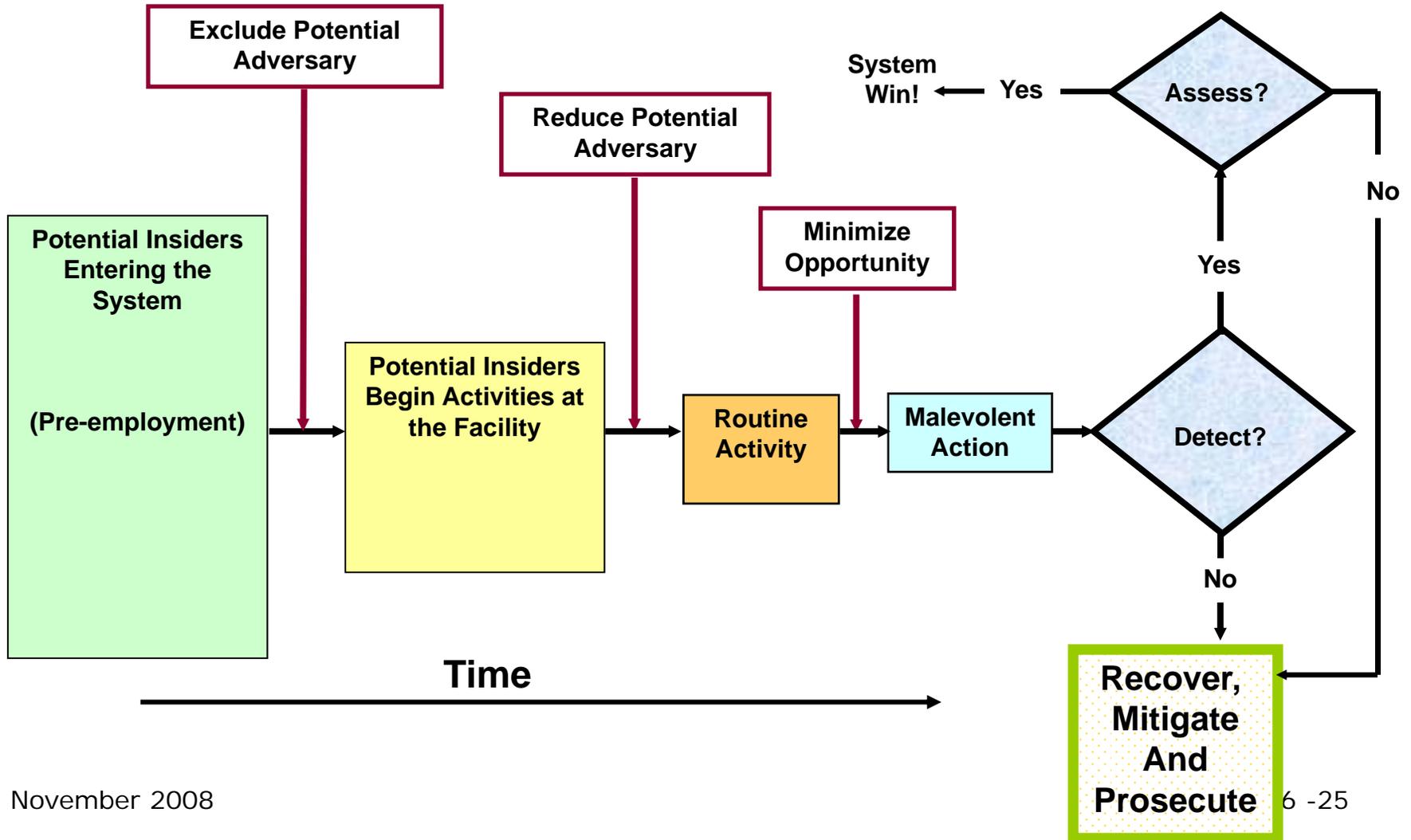


Protective Force monitors and conducts searches at entry/exit control points at each layer of a facility providing detection and assessment capability against insider theft attempts.

Protective Force monitors alarms and cameras providing protection and surveillance of nuclear materials.



# Insider Protection System Approach



# Recovery, Mitigate, and Prosecute

---

- **Response if malevolent action is not prevented or action / consequence is detected late**
  - **Recovery includes retrieval of stolen or diverted material**
    - Physical inventories will need to be performed
  - **Mitigation includes actions that will minimize the consequences (sabotage)**
  - **Prosecution of adversary**
    - Provides justice
    - Deters others by demonstrating penalties
    - Establishes the resolve to address insider problems
  - **Adjust system to react more favorably based on lessons learned**



# Video Exercise

---

- **Watch the video and observe safeguard elements associated with detection and assessment**
- **Discussion**

# Module Summary

---

- **Identify detection elements**
  - Timely
  - Late
- **Identify assessment elements**
- **Identify the administrative and technical measures in a MPC&A system that can provide detection and assessment against an insider threat**
- **Video Exercise**

**Questions or Comments??**





# Lecture 7

## Quantifying Late Detection in MC&A



Lawrence Livermore  
National Laboratory



# Learning Objective

---

- **Understand the concept of late detection**
- **Review the statistics used in MC&A**
- **Specify the Pd and timelines for Pd for MC&A elements for item inventories**
- **Review elements of process control (e.g., limits of error on the inventory difference) as they relate to bulk processes.**
- **Specify the timelines and detection thresholds for Pd for MC&A elements for bulk or Processing Operations**

# Late Detection – Is it late?

---

- **Classic Definition**

“When detection occurs too late to prevent a **theft**, it is called a late detection or late alarm. Activities or events that may provide late detection usually belong to material control and accountability (MC&A) activities ”

(Evaluating late detection capability against diverse insider adversaries - [Sicherman, A.](#) Lawrence Livermore National Lab., CA (USA) Transactions of the American Nuclear Society ; Vol/Issue: 55; 3. international conference on facility operations safeguards interface; 29 Nov - 4 Dec 1987; San Diego, CA (USA); DOE Project)

# A better definition???

---

“When detection occurs too late to prevent a **theft of a significant quantity**, it is called a late detection or late alarm. Activities or events that may provide late detection usually belong to material control and accountability (MC&A) activities ”

**So sometimes maybe MC&A isn't really late at all???**

---

**Discussion –**

**Contrasting with other common examples**

# Correct words?

---

- **MC&A Delayed but soon enough detection**
  - Identifies the anomaly
  - Identifies it before it becomes significant
  - Enables corrective actions to be implemented.

# Statistics used in Safeguards

---

- **Sampling and inspection plans**
  - **Attributes or acceptance sampling plans where the population,  $N$ , is unacceptable, if one or more defects is found in a sample of size  $n$**
- **Process Control**
  - **Measurements or Measurement control**
  - **Standards and Traceability**
  - **Quantifying the error of measurement**
  - **Effect of measurement error on Safeguards decisions (e.g., Material balance or inventory difference evaluation)**
  - **Controlling and reducing the error of measurement**



# Lecture 7.1

---

## Quantifying Late Detection in MC&A for item inventories



# Learning Objective

---

- 1. Understand how physical inventories, sampling plans, and other checks of the inventory factor into detection of insider activity.**
- 2. Be able to quantify the probability of detection for various scenarios in a single inventory and over several inventories.**
- 3. Understand how physical inventory and sampling procedures relate to the assumptions, analysis, and scenarios in the vulnerability assessment.**

# **If Insider selects the item inventory as their target, a defect will be introduced into the inventory**

---

**Ability and probability to detect a given defect depends upon several things:**

- 1) How the item is inspected (e.g., inspection procedure)**
  - a) Item Count**
  - b) Inventory by serial number and location**
  - c) Confirmatory measurement**
  - d) Verification measurement**
- 2) Number of defects (e.g., 1 item or several items)**
- 3) Number of items inspected during each inventory**
- 4) Frequency of inspections (timeliness of detection)**

# Types of inspections and scenarios they can detect:

---

- **Item count**
  - **Missing item**
- **Inventory by serial number, seal, and location**
  - **Missing item by serial number**
- **Confirmatory measurement (weight and/or some other attribute)**
  - **Tampering with item and some substitution scenarios**
- **Verification measurement**
  - **Material removal (within limits of measurement) and substitution scenarios**

# Relationship to the Vulnerability Assessment

---

- **Number of defects is related to the goal quantity**
- **Type of inspection is directly related to insider scenario one is trying to detect**
- **Probability of detection from the Material Accounting is a statistical calculation based on the two preceding bullets**

# Sampling Formula for required sample size

---

$$n = (N - d/2)(1 - \beta)^{1/(d+1)}$$

**N = Population Size**

**$\beta$  = specified probability of failing to find at least one critical nonconformity**

**d = maximum number of critical non-conforming items “allowed” in the lot or population.**

**n = sample size**

## What if the “Goal Quantity” is 3 items

| Goal Quantity = 3 items and chance of finding at least one defect 90% |   |         |                  |
|---|---|---------|------------------|
| N   | d | $\beta$ | n or sample size |
| 100   | 3 | 0.1     | 43               |
| 200   | 3 | 0.1     | 87               |
| 1000  | 3 | 0.1     | 437              |
| Goal Quantity = 3 items and chance of finding at least one defect 95% |   |         |                  |
| N   | d | $\beta$ | n or sample size |
| 100   | 3 | 0.05    | 52               |
| 200   | 3 | 0.05    | 105              |
| 1000  | 3 | 0.05    | 526              |
| Goal Quantity = 3 items and chance of finding at least one defect 99% |   |         |                  |
| N   | d | $\beta$ | n or sample size |
| 100   | 3 | 0.01    | 67               |
| 200   | 3 | 0.01    | 136              |
| 1000  | 3 | 0.01    | 683              |

# What if the "Goal Quantity" is 1 item

| Goal Quantity = 1 item and chance of finding at least one defect 90% |   |         |                  |
|--|---|---------|------------------|
| N  | d | $\beta$ | n or sample size |
| 100  | 1 | 0.1     | 68               |
| 200  | 1 | 0.1     | 136              |
| 1000   | 1 | 0.1     | 683              |

| Goal Quantity = 1 item and chance of finding at least one defect 95% |   |         |                  |
|--|---|---------|------------------|
| N  | d | $\beta$ | n or sample size |
| 100  | 1 | 0.05    | 77               |
| 200  | 1 | 0.05    | 155              |
| 1000   | 1 | 0.05    | 776              |

| Goal Quantity = 1 item and chance of finding at least one defect 99% |   |         |                  |
|--|---|---------|------------------|
| N  | d | $\beta$ | n or sample size |
| 100  | 1 | 0.01    | 90               |
| 200  | 1 | 0.01    | 180              |
| 1000   | 1 | 0.01    | 900              |

# What if the "Goal Quantity" is "0" Defects?

| Zero defects at 90% |   |         |                  |
|---------------------|---|---------|------------------|
| N                   | d | $\beta$ | n or sample size |
| 100                 | 0 | 0.1     | 90               |
| 200                 | 0 | 0.1     | 180              |
| 1000                | 0 | 0.1     | 900              |
| Zero defects at 95% |   |         |                  |
| N                   | d | $\beta$ | n or sample size |
| 100                 | 0 | 0.05    | 95               |
| 200                 | 0 | 0.05    | 190              |
| 1000                | 0 | 0.05    | 950              |
| Zero defects at 99% |   |         |                  |
| N                   | d | $\beta$ | n or sample size |
| 100                 | 0 | 0.01    | 99               |
| 200                 | 0 | 0.01    | 198              |
| 1000                | 0 | 0.01    | 990              |

# What happens over time (e.g., delayed detection from repeated inspections)?

---

**Russian Roulette example:**

**If you play consecutive games of roulette, including spinning the cylinder between each time, you have 5/6th of a chance of surviving every time - 83.3 %.**

**Doesn't sound so bad?**

**But what happens if you keep going?**

# Statistics behind Russian Roulette

---

(Probability of surviving)<sup>number of games</sup>

- **Game 1 – (Probability of surviving)<sup>1</sup>**
- **Game 2 – (Probability of surviving)<sup>2</sup>**
- **Game 3 – (Probability of surviving)<sup>3</sup>**
- **Game 4 – (Probability of surviving)<sup>4</sup>**
- **Game 5 – (Probability of surviving)<sup>5</sup>**
- **Game 10 – (Probability of surviving)<sup>10</sup>**
- **Game 20 – (Probability of surviving)<sup>20</sup>**
- **Game 50 – (Probability of surviving)<sup>50</sup>**

# Russian Roulette - Continued

---

- After 1 game, you have 83.33% chance of still being alive
- After 2 games, you have 69.44% chance of still being alive
- After 3 games, you have 57.87% chance of still being alive
- After 4 games, you have 48.22% chance of still being alive
- After 5 games, you have 40.19% chance of still being alive
- After 10 games, you have 16.15% chance of still being alive
- After 20 games, you have 2.61% chance of still being alive
- After 50 games, you have 0.011% chance of still being alive

**In other words: after 4 games, chances are less than 50/50 for still being alive. Perhaps it might be better to play a game of poker instead.**

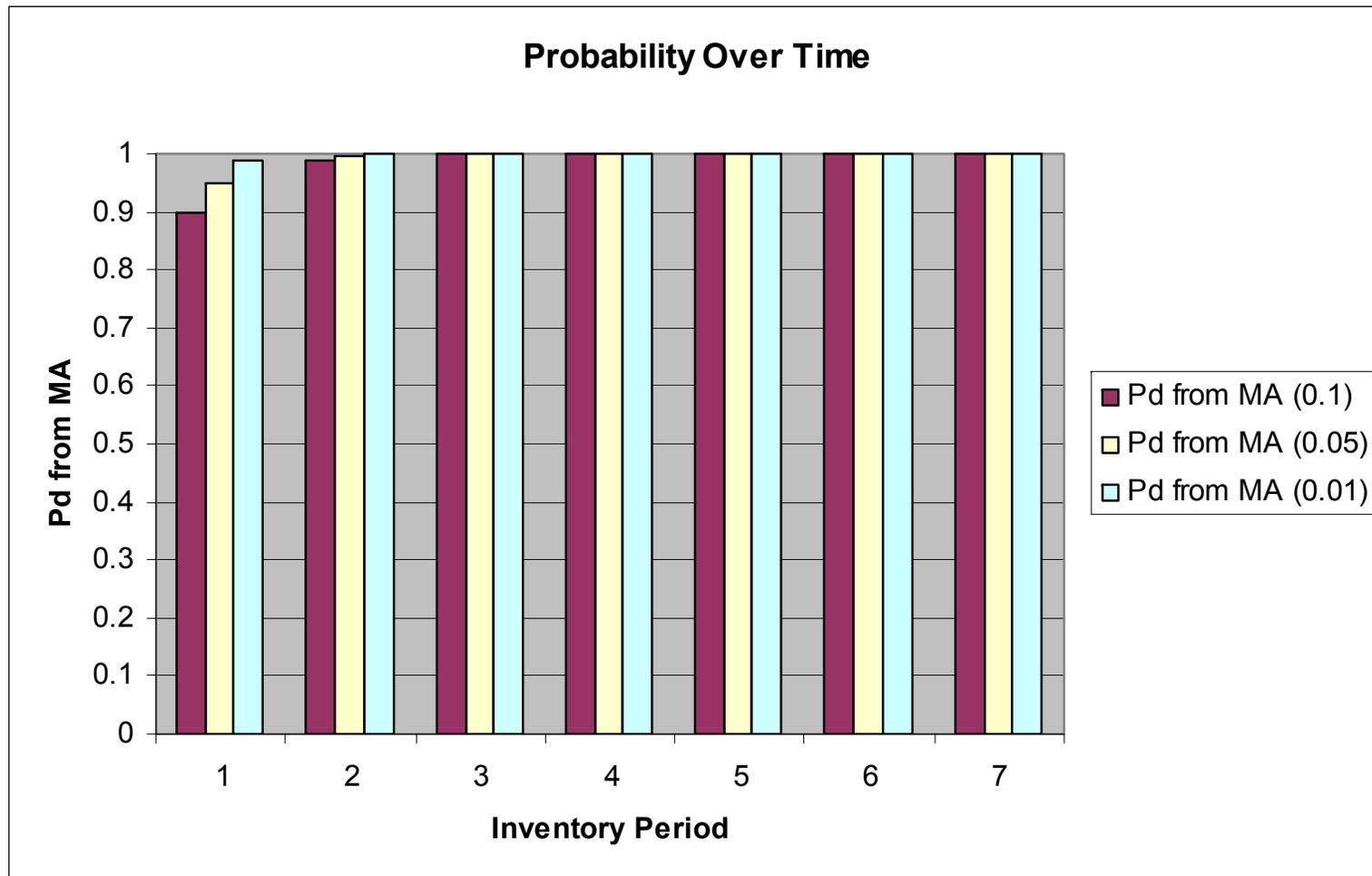
# Multiple Inventory Periods (note: for example use $\beta = .10$ )

---

$P^{\text{Number of Inventories}}$

- **After one inventory insider has a 0.10 probability of escaping detection.**
- **After two inventories insider has a 0.01 probability of escaping detection.**
- **After 3 inventories insider has a 0.001 probability of escaping detection and so on.....**

# Probability of detection from Material Accounting over time at various inspection levels



# Exercises

---

- 1. Small Group – See handout**
- 2. Large Group – Simulated inventory with defects**



## Lecture 7.2

---

# Quantifying Late Detection in MC&A for Bulk Processes



# Learning Objective

---

- **Familiarization with the probability with which the Safeguards systems can detect a diversion of material due to insider activity**
- **Become familiar with the concept of Statistical Process Control**

# Material Balance Evaluation from the Insider Perspective

---

- **Goal is determine the probability with which the Safeguards systems can detect a diversion of material due to insider activity.**
- **Generally relates to bulk processing.**
  - “Bulk Material – Material in any physical form that is not identifiable as a discrete item and therefore must be accounted for by weight, volume, sampling, chemical analysis, or non-destructive analysis”
- **Statistical Process Control is the key underlying concept or discipline**

# Overview

---

- **Inventory differences (IDs)**
- **Process Control – statistical methods and control charts**
- **Discuss with respect to the hypothetical process**
- **Discuss the calculation of Limits-of-Error for inventory differences (LEIDs)**

# Inventory Difference Calculation

---

The ID is calculated as follows:

$$\text{ID} = \text{BI} + \text{TI} - \text{TO} - \text{EI}$$

Where,

**ID** = Inventory Difference

**BI** = Beginning Inventory (prior period physical inventory value)

**TI** = Transfers In (additions) during the current inventory period

**TO** = Transfers Out (removals) during the current inventory period

**EI** = Ending Inventory (current period physical inventory value )

# Inventory Differences

---

- For an item facility, the ID should always be zero unless an item is missing.
- For a bulk facility,
  - The ID is typically different from zero due to measurement uncertainties, unmeasured holdup, and losses.
  - The holdup can be treated by estimating the amount in various pieces of equipment, perhaps based on experiments.
  - Under ideal conditions, the bulk facility IDs should vary about zero. (note: systematic differences may cause this not to be the case).

# Simplified ID Example for an Item Facility

---

**Reactor Core:**

**BI = 60 core fuel assemblies**

**TI = 20 fresh fuel assemblies**

**TO = 20 spent fuel assemblies**

**EI = 60 core fuel assemblies**

$$\mathbf{ID = 60 + 20 - 20 - 60 = 0}$$

# Simplified ID example for a bulk facility

---

## Fabrication Plant Process Area:

**BI = 203.5 kg U in beginning process inventory**

**TI = 600.1 kg U in oxide powder feed**

**TO = 604.8 kg U in pellet product**

**EI = 195.6 kg U in ending process inventory**

**ID = 203.5 + 600.1 - 604.8 - 195.6 = 3.2 kg U**

# Making sense of the ID with respect to the Insider

---

- **What techniques can be used to monitor it?**
- **How does it relate to the insider analysis in the vulnerability assessment?**
- **When is it or how much of an ID is significant?**

## **MOST IMPORTANTLY....**

- **What are we trying to detect?**

# What is significant? Was 3.2 kg from the example in a previous slide significant?

---

| Process A – Not significant |            |    | Process B - Significant |            |    |
|-----------------------------|------------|----|-------------------------|------------|----|
| Inventory                   | Period     | ID | Inventory               | Period     | ID |
| 1                           | -1.5       |    | 1                       | -.15       |    |
| 2                           | 2.3        |    | 2                       | .23        |    |
| 3                           | -3.1       |    | 3                       | -.31       |    |
| 4                           | 0.7        |    | 4                       | 0.07       |    |
| <b>5</b>                    | <b>3.2</b> |    | <b>5</b>                | <b>3.2</b> |    |
| 6                           | -0.8       |    | 6                       | -.08       |    |
| 7                           | -1.6       |    | 7                       | -.16       |    |
| 8                           | -0.6       |    | 8                       | -.06       |    |
| 9                           | 1.1        |    | 9                       | .11        |    |
| 10                          | 2.1        |    | 10                      | .21        |    |
| 11                          | -3.2       |    | 11                      | -.32       |    |
| 12                          | 1.5        |    | 12                      | .15        |    |

# What about process C? Significant significant?

---

| Process C – Not significant |            |
|-----------------------------|------------|
| Inventory                   | Period ID  |
| 1                           | -1.0       |
| 2                           | 2.0        |
| 3                           | -1.5       |
| 4                           | 0.7        |
| <b>5</b>                    | <b>3.2</b> |
| 6                           | -0.8       |
| 7                           | -1.3       |
| 8                           | -0.6       |
| 9                           | 0.7        |
| 10                          | 1.5        |
| 11                          | -2.1       |
| 12                          | 1.2        |

# Key concepts

---

- **What are we trying to detect?**
  1. **Single abnormally large or statistically significant inventory difference**
  2. **Repetitive losses over time that could indicate insider activity**
- **How will they manifest themselves?**
  - **Large loss similar to Process B in the previous slide for the single occurrence.**
  - **Repetitive losses over time or in laymen's terms a loss trend or in statistical terms is a shift in the mean of the inventory difference over time**

# Process or Product Monitoring and Control

---

- **Shewart Control Charts**
- **Cumulative Sum (CUSUM) Control Charts**
- **Exponentially Weighted Moving Average (EWMA) Control Charts**
  
- **MOST IMPORTANT PART**
  - **Average Run Length (ARL)**
    - **When the process is operating at the target mean and a shift of magnitude  $\delta$  occurs the number of inventories it takes to detect the shift.**
  - **Generally CUSUM or EWMA are better at 2 sigma or less while Shewart is better at greater than 2 sigma.**

# Average Run Length to detect a 1 sigma shift in the process average for the various techniques

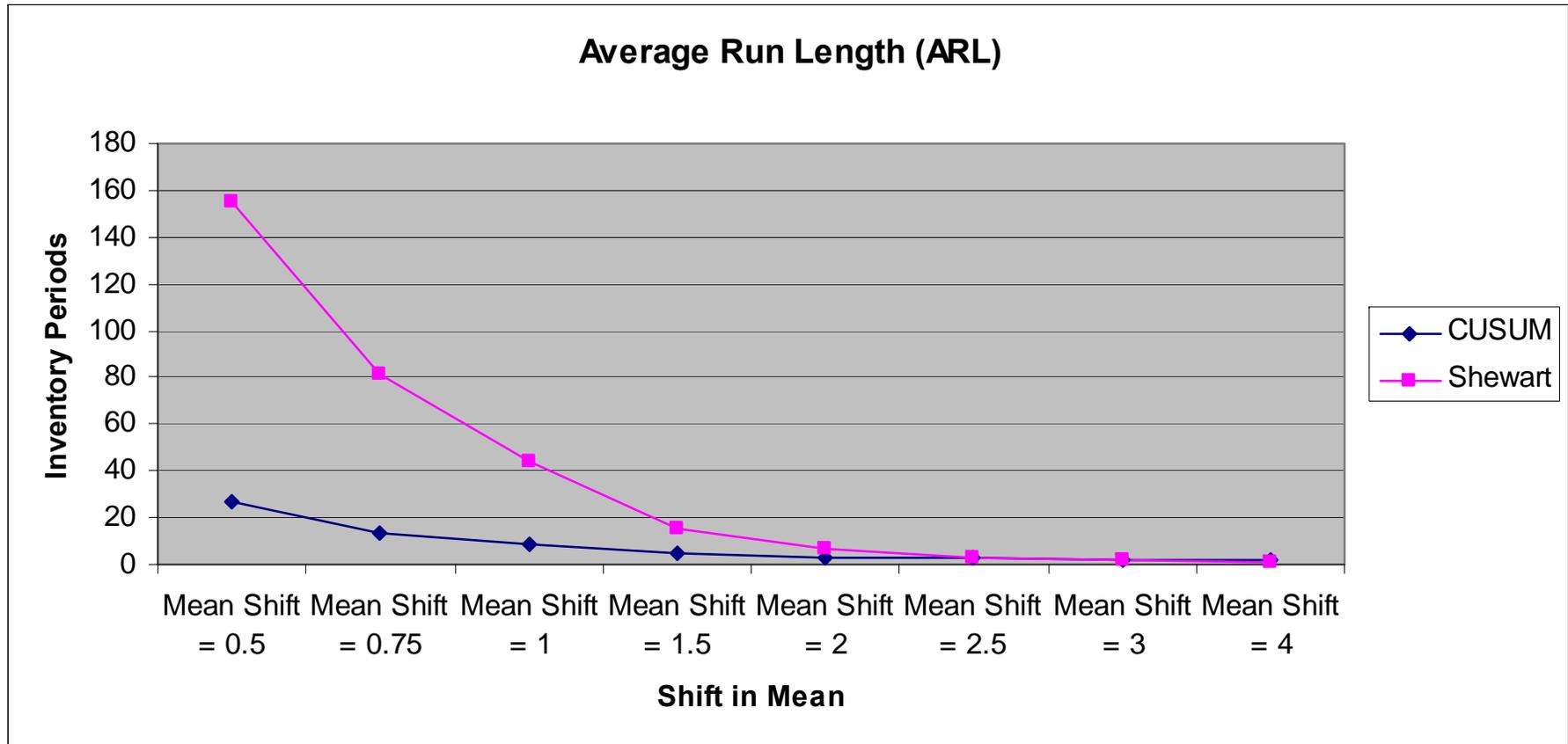
---

- **Shewart Charts will detect a 1 sigma (standard deviation) shift in the mean in around 42-44 inventories**
- **Both CUSUM and EWMA will detect a 1 sigma shift in about 10 inventories**
- **As the shift in the mean gets smaller all techniques converge on 370 inventories**
- **As the shift in the mean gets larger (e.g., around 2.5 sigma or greater) Shewart is more effective**

**Note: Under current DOE regulations an ID > 2 sigma (warning limit) will be investigated regardless.**

# Average Run Length (ARL)

## CUSUM versus Shewart based on shift in process mean



# Average Run Length (ARL)

## CUSUM versus Shewart based on shift in process mean

| Shift in Mean ( $\delta$ )<br>(k=0.5) | CUSUM<br>(h=4) | Shewart |
|---------------------------------------|----------------|---------|
| 0.5                                   | 26.6           | 155     |
| 0.75                                  | 13.3           | 81      |
| 1.0                                   | 8.38           | 44      |
| 1.5                                   | 4.75           | 14.97   |
| 2                                     | 3.34           | 6.3     |
| 2.5                                   | 2.62           | 3.24    |
| 3                                     | 2.19           | 2       |
| 4                                     | 1.71           | 1.19    |

# Shewart Charts

---

- **First proposed by during the 1920's by Dr. Walter A. Shewart**

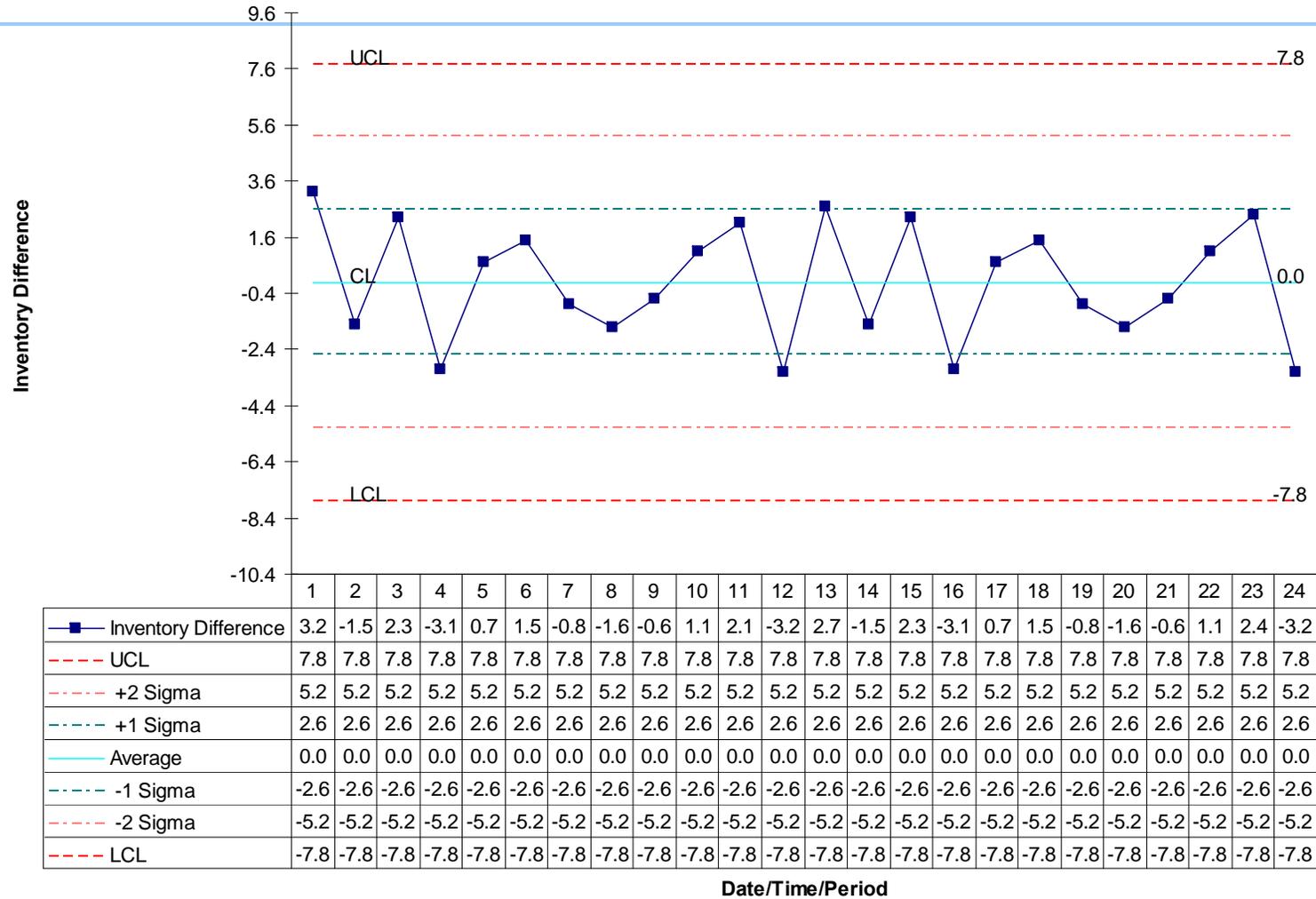
**UCL = Process Mean + k (standard deviation)**

**Center Line = Process Mean or target**

**LCL = Process Mean – k (standard deviation)**

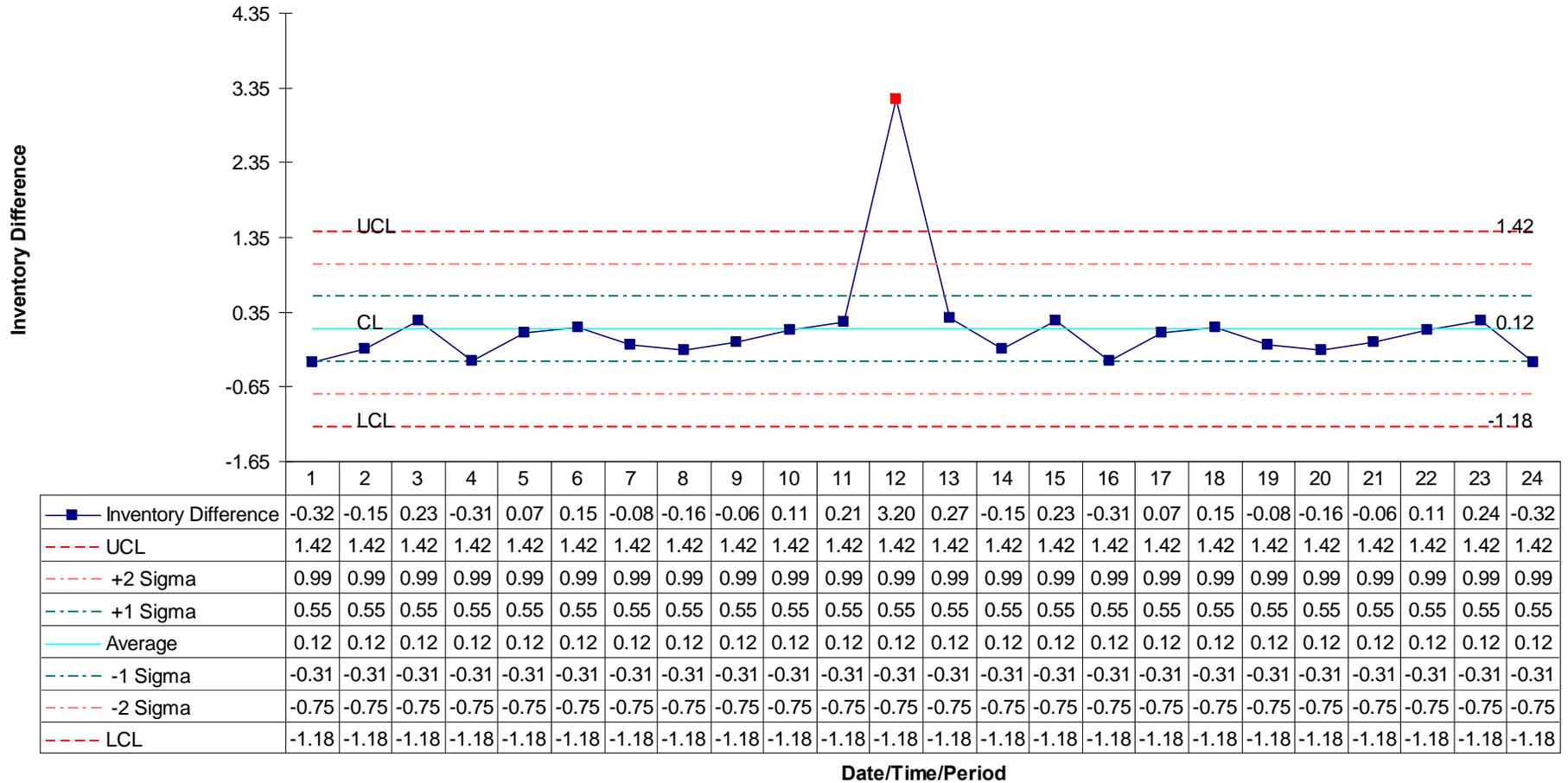
# Shewhart Chart for Process A

Inventory Difference X



# Shewhart Chart – Process B

Inventory Difference X



# Shewart Charts

## Advantages/Disadvantages

---

### Advantages

- **Very effective at detecting large process shifts**

### Disadvantages

- **Not so good for trends because it only uses information contained in the last data point**

**Can address some of the disadvantages with respect to trends by apply the Western Electric Company Rules (WECO) for signaling out of control situations.**

# WECO Rules for evaluating Shewart Charts

---

- Any point above +3 sigma
- 2 out of the last 3 points above +2 sigma
- 4 out of the last 5 points above +1 sigma
- 8 consecutive points on the positive side of the center line
- 8 consecutive points on the negative side of the center line
- 4 out of the last 5 points below -1 sigma
- 2 out of the last 3 points below -2 sigma
- Any point below -3 sigma

**Note:** Under current DOE regulations an ID > 2 sigma (warning limit) will be investigated regardless.

# Cumulative Sum (CUSUM) Charts

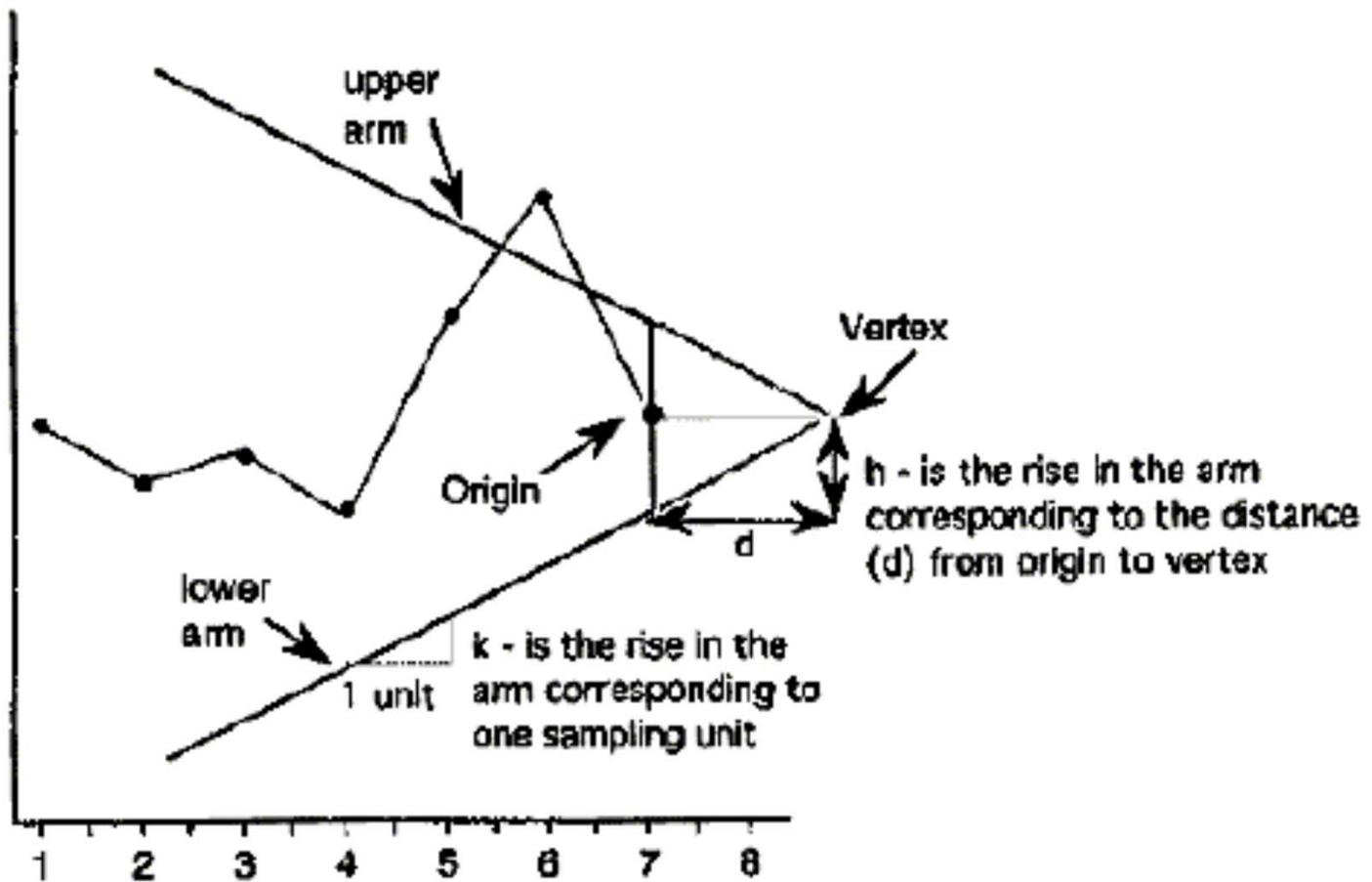
---

- The control chart is formed by plotting the cumulative sums of the difference between the current data and the target value of the “in-control” process.
- The cumulative sum response ( $S_t$ ) for a control chart is calculated using the equation at the right where  $\bar{X}_i$  is the subgroup mean and  $\mu_0$  is the target value and  $\sigma_x$  is the standard deviation.

$$S_t = \sum_{i=1}^t \left( \frac{\bar{X}_i - \mu_0}{\sigma_{\bar{X}_i}} \right)$$

# CUSUM with an sample V-Mask demonstrating an out of control process

*Sample V-Mask demonstrating an out of control process*



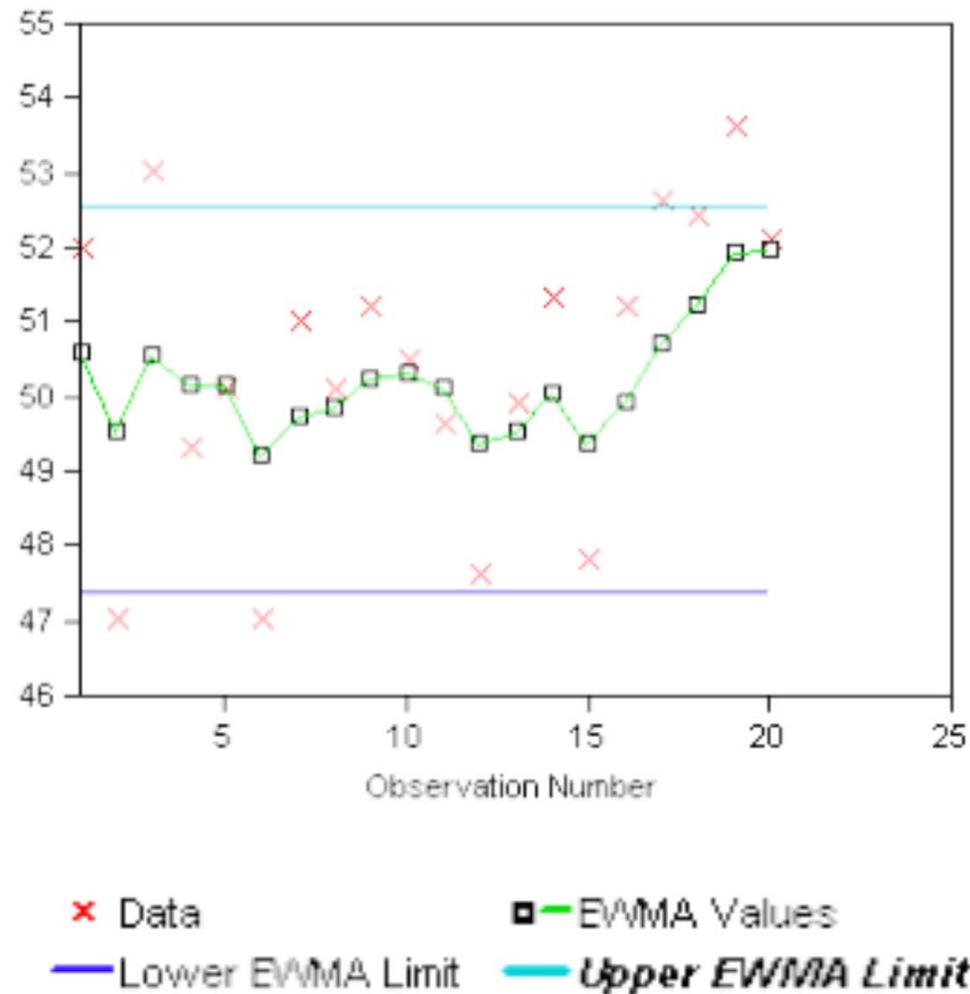
# Exponentially Weighted Moving Average (EWMA) Control Charts

---

- Uses a weighting factor  $r$  ( $0 < r \leq 1$ ) which decreases measurement weighting exponentially going backwards in time.
- It is calculated using the equation at the right where  $\bar{X}_i$  is the current observation and  $r$  is the weight assigned to the most recent measurement.
- A small value of  $r$  guards against a small shift in the mean.

$$EWMA_t = \sum_{i=1}^t r(1-r)^{t-i} \bar{X}_i$$

# EWMA Chart example showing in-control but a trend in the process



# CUSUM and EWMA Charts

## Advantages/Disadvantages

---

### Advantages

- **Very effective at detecting small process shifts**

### Disadvantages

- **Not as effective as Shewart charts (e.g., 2 sigma or greater)**
- **CUSUM is not as intuitive and generally requires specialized software**

# EXERCISE

---

- **Simulate various theft scenarios and how the charting techniques react.**

# Summary

---

- **Process shifts in the inventory of 2 sigma or greater are relatively easy to detect (e.g., significant statistically) within 1 inventory period**
  - Shewart charting approach most effective
- **Process shifts in the inventory of 1-2 sigma will be detected within 10 inventory periods**
  - CUSUM or EWMA tend to be more effective although Shewart with WECO rules applied can be effective
- **Process shifts in the inventory of 0-1 sigma, while not be statistically significant may be seen using the techniques discussed previously (*note: timeline for Pd variable*)**



## Lecture 7.3

---

# Hypothetical Facility Bulk Processes and Late Detection



# Learning Objective

---

- **Explain the difference between control limits and specification limits**
- **Understand the concept of process capability from a regulatory perspective and as it applies to the hypothetical facility**
- **Explain strategies of process control for nuclear process and the relationship of MC&A and PP within these strategies**

# Overview

---

- **Process Capability**
- **Process capability with respect to the hypothetical facility**
- **Strategies for improving the process capability**
- **Relationship of MC&A and PP with respect to process capability**

# What are the differences between control limits and specification limits?

---

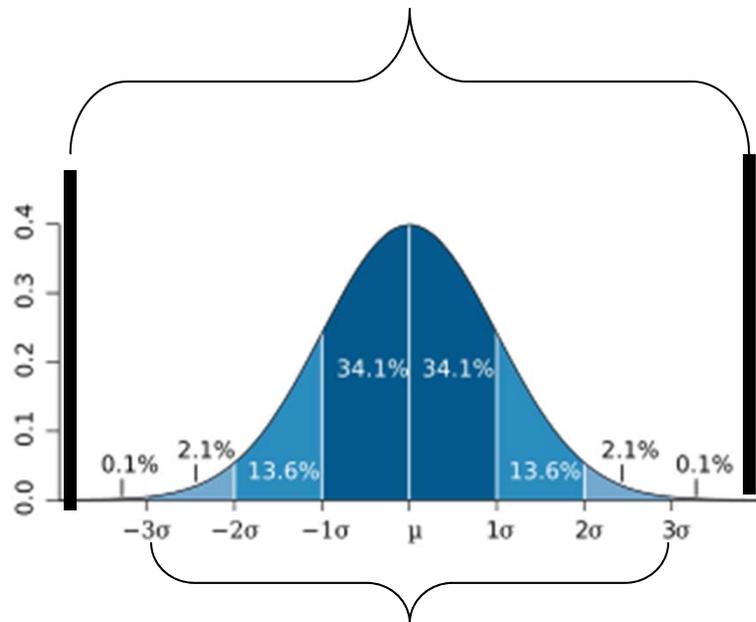
- **Control Limits** are used to determine if the process is in a state of statistical control.
- **Specification Limits** are used to determine if the product will function in the intended fashion.

**Note:** In another lecture we will discuss the concept of **Specification Limits** with respect to **Significant Safeguards Limits** and introduce a concept called **Process Capability**.

# Process Capability considers process variability relative to specifications to determine if the process is "capable"

## Very Capable

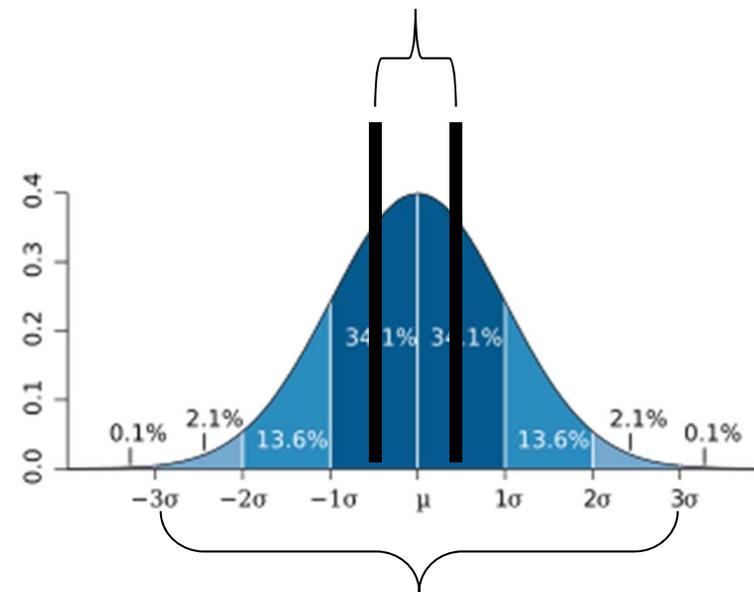
Safeguards Limits or what we would like to detect



Due to process uncertainty what we can detect.

## Not very capable

Safeguards Limits or what we would like to detect



Due to process uncertainty what we can detect.

# Process Capability Performance Requirements from the regulatory basis

---

- **2 sigma limits should be no greater than 2% of active inventory (def. Sum of beginning inventory, additions, ending inventory, and removals). (DOE and Russia's OPUK)**
- **For U235 >20% enrichment this should not exceed 8 kg.**
- **Control Limits or Specification Limits??**

# Hypothetical Facility Specification Limits

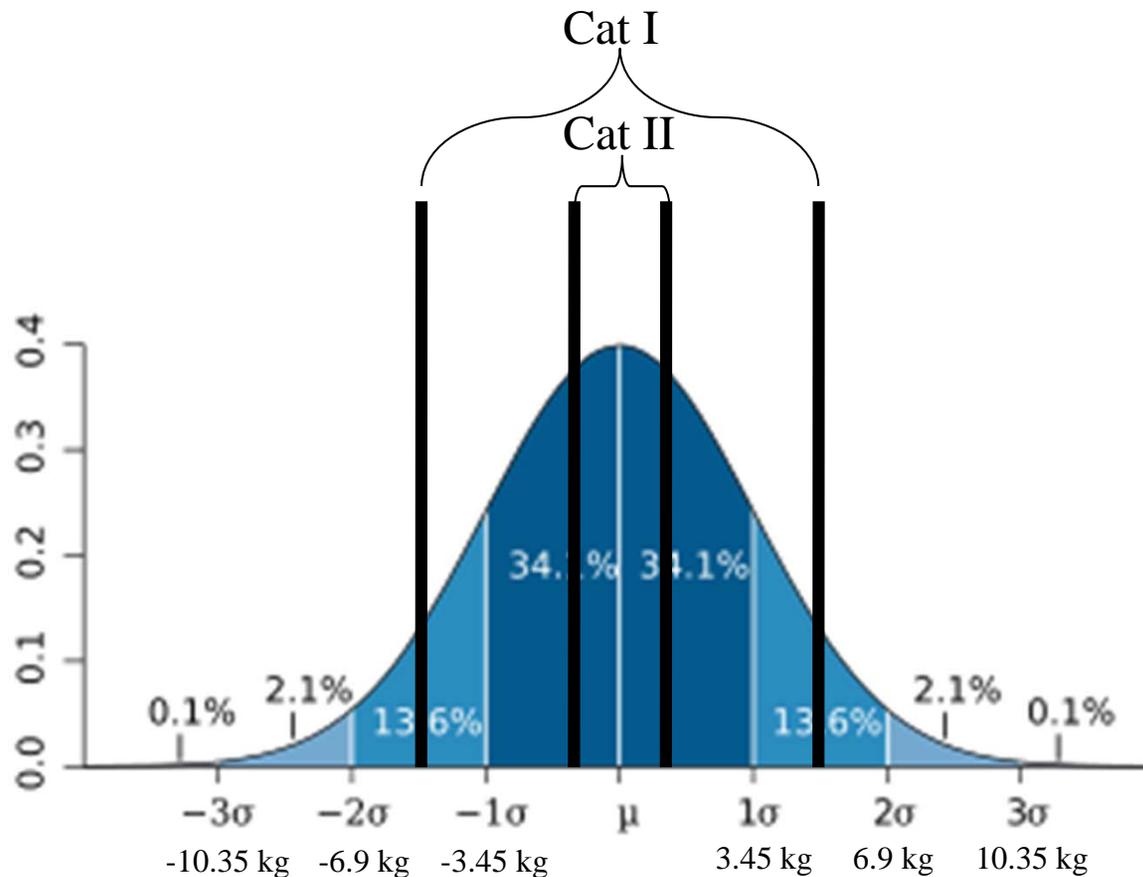
---

**Active Inventory**                      **393 kg**

**2%**    **6.9 kg**

**Summary – in theory the Hypothetical Facility should be just within the regulatory performance requirement. This is not the actual performance but the just the performance requirement or specification limit based on the regulations. Actual performance can be better or worse.**

# Hypothetical Facility Graph showing Category I (5 kg) and II (1 kg) limits for U235 metal



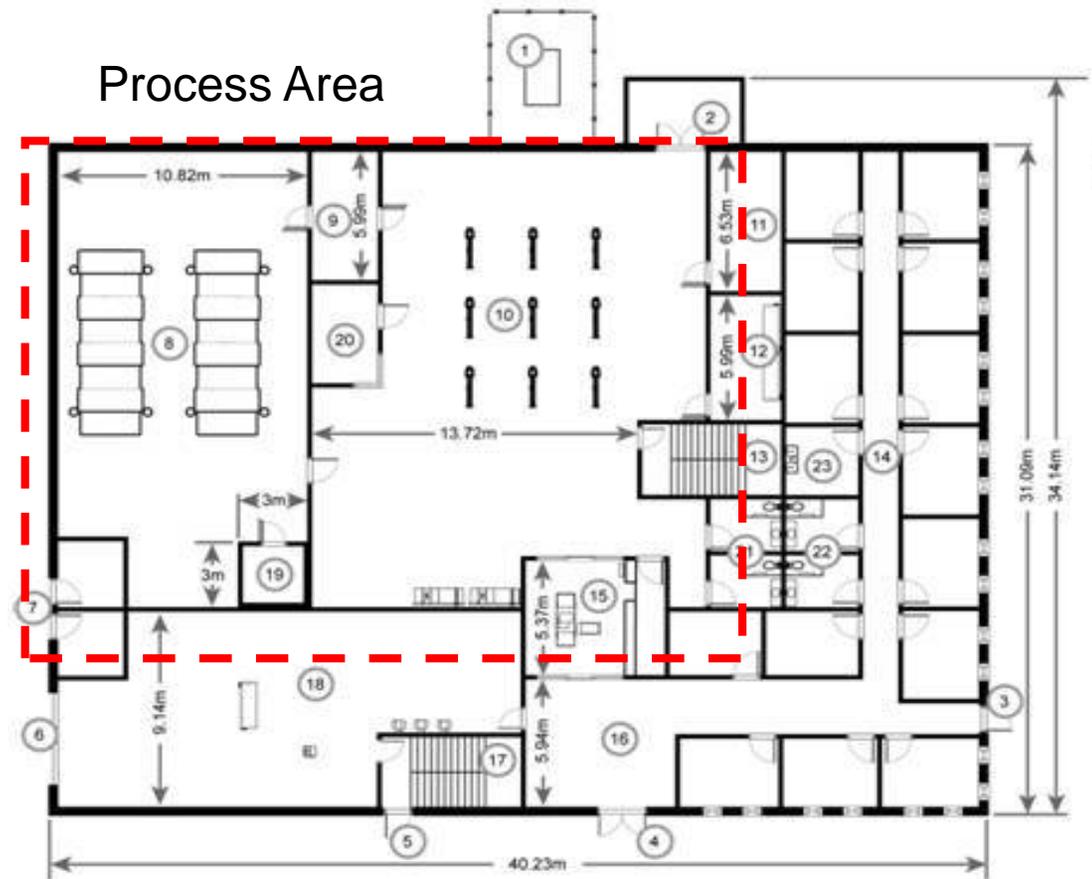
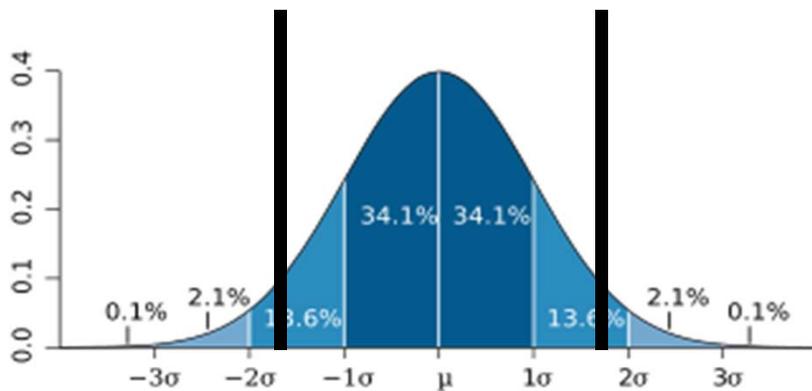
# Structure of Material Balance Areas Regulatory Requirement

---

**A facility should have at least one or more material balance areas. The MBAs should be structured such that inventory differences are localized and the uncertainty on the inventory difference is minimized**

# Hypothetical Facility

Limit of Error on the Inventory Difference  
for the whole process

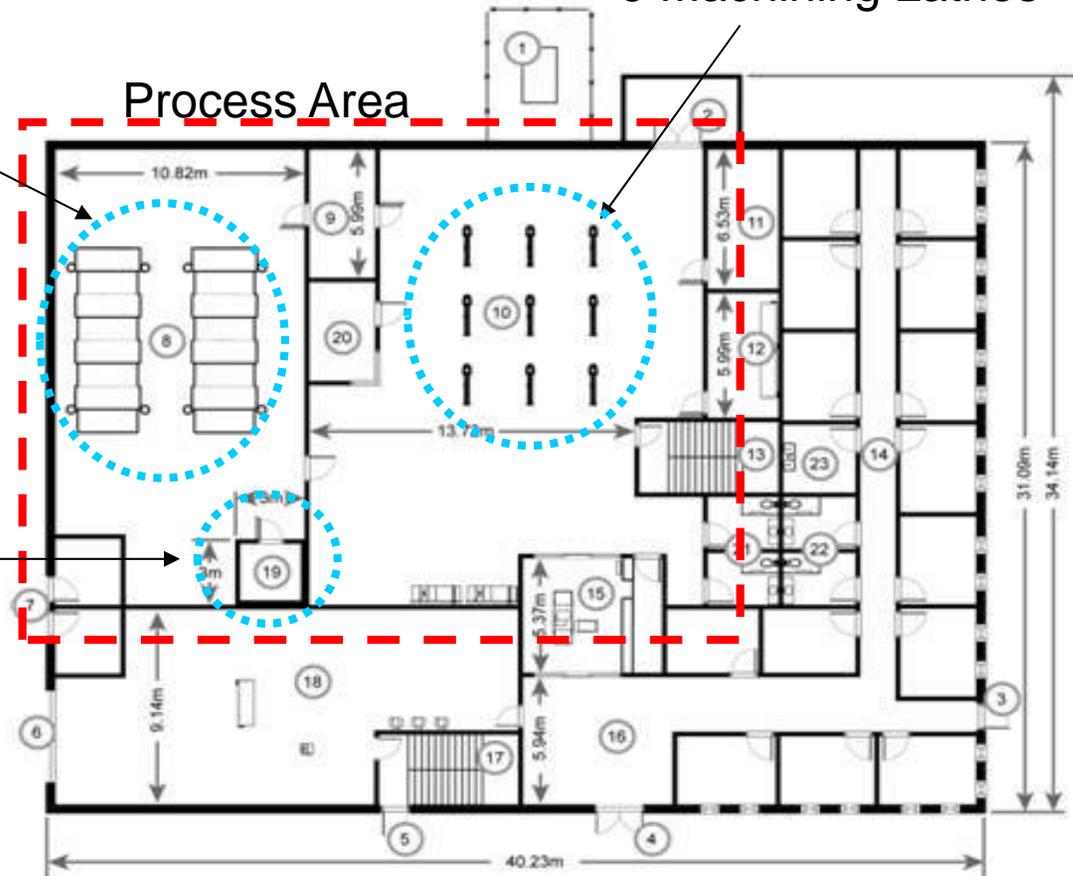


# Hypothetical Facility and the Process Subparts

2 Casting Furnaces

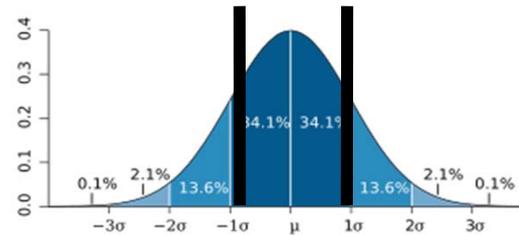
9 Machining Lathes

1 vault containing Charge (for casting) make-up area

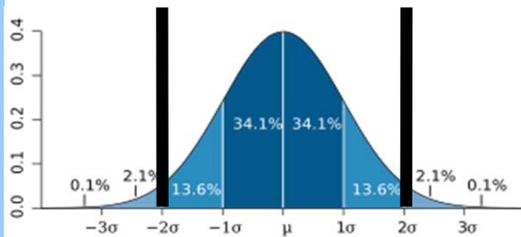


# Hypothetical Facility and the Process Subparts

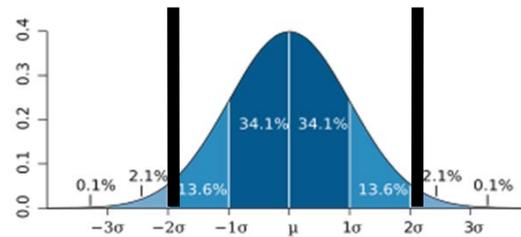
Total Process



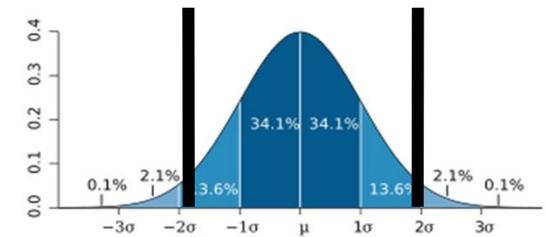
9 Machining Lathes



2 Casting Furnaces

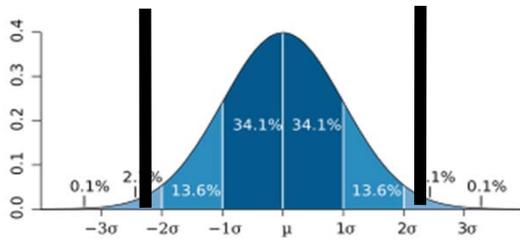


1 vault containing Charge (for casting) make-up area

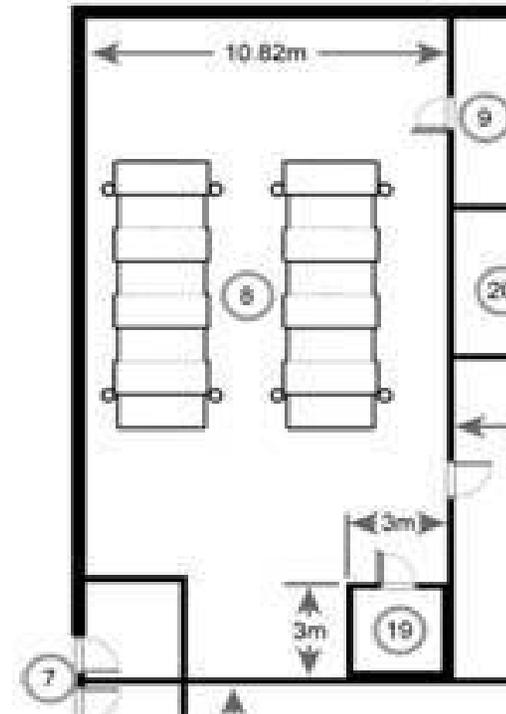
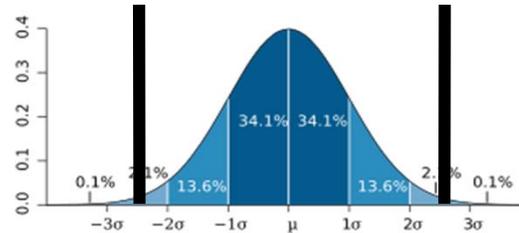


# Hypothetical Facility and Casting Area

2 Casting Furnaces



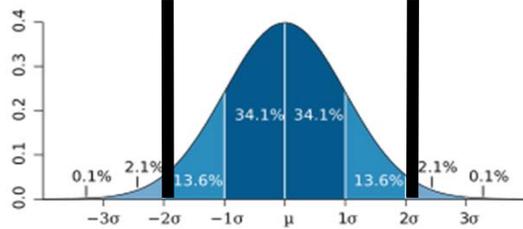
1 vault containing  
Charge (for casting)  
make-up area



# Hypothetical Facility and Machining Area

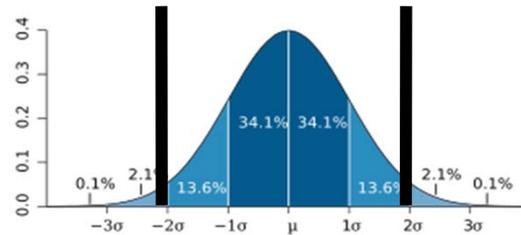
## Can it be broken down further?

9 Machining Lathes

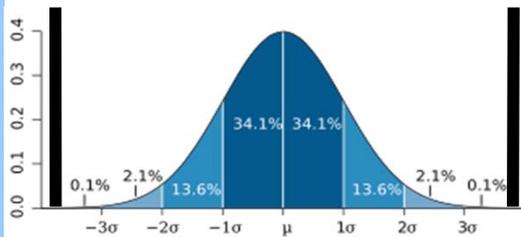


# Machining Lathes can be subdivided

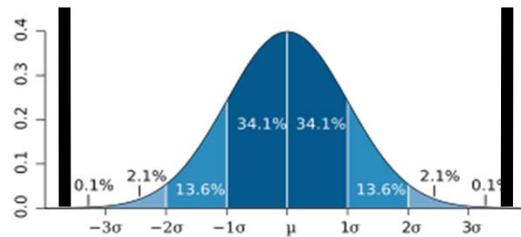
## 9 Machining Lathes



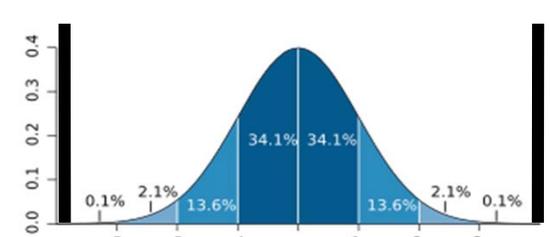
Lathe 1



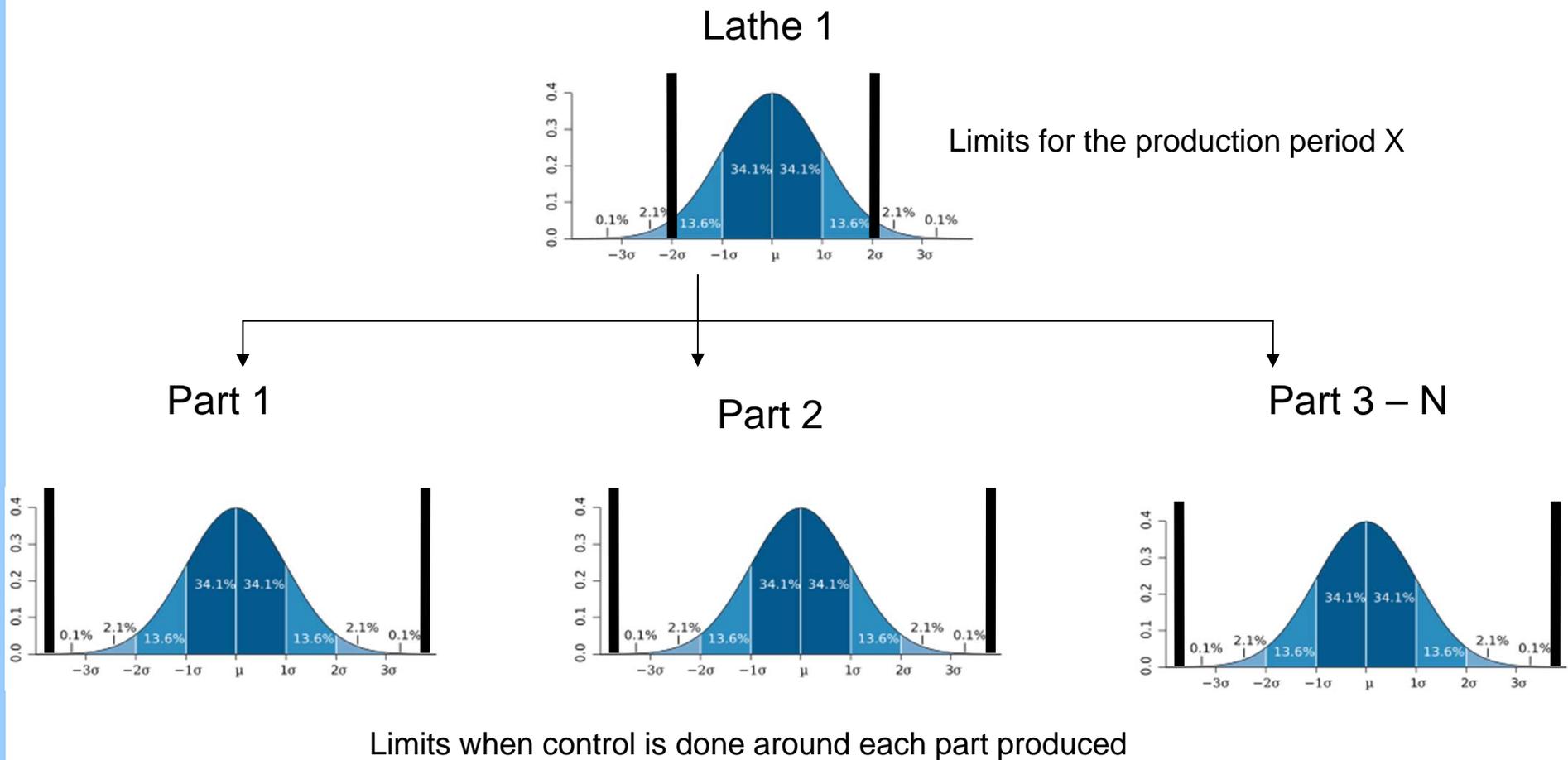
Lathe 2



Lathe n – Etc.



# What happens under processing monitoring



# How do MC&A and Physical Protection work together?

---

- **MC&A establishes an MBA structure and process control methodology that localizes inventory differences and maximizes the ability to detect process shifts of safeguards significance**
- **Physical Protection controls access and enforces separate of duties to minimize credible scenarios (e.g., access, knowledge, and authority) where an insider can circumvent the MC&A controls**



# Lecture 7.4

---

## Establishing Control Limits



# Learning Objective

---

- **Explain the difference between control limits and specification limits.**
- **Be able to discuss methods for calculating control limits.**
- **Complete a simple Propagation of Variance**
- **Explain strategies of process control for nuclear process and the relationship of MC&A and PP within these strategies.**

# Overview

---

## The Calculation of Limits-of-Error for Inventory Differences (LEIDs)

# What are the differences between control limits and specification limits?

---

- **Control Limits** are used to determine if the process is in a state of statistical control.
- **Specification Limits** are used to determine if the product will function in the intended fashion.

# **Material Balance Evaluation**

## **Combining errors or establishing control limits**

---

**In safeguards, we are often asked the uncertainty in a value that results from combining two or more measured values:**

- **Calculating mass of nuclear material from measurements  
(weight and concentration, for example)**
- **Shipper receiver difference (SRD)**
- **Remeasurement (are two different measured values for the same item within measurement uncertainty)**
- **Material balance (e.g., inventory difference)**

# Material Balance Evaluation

## Combining errors

---

- **First step is to determine how measured values are combined**
- **The following are examples of equations used to combine the measured values**
  - **Mass (M) = Net Weight \* Concentration**
  - **Shipper/receiver difference (SRD) =**  
**Shipper's value – Receiver's value**
  - **ID = BI + TI - TO - EI**

# Material Balance Evaluation

## Combining errors

---

- **Second step is to determine how errors combine**
  - **Variances combine, not standard deviations**
  - **Error models**
  - **Random and systematic errors**
  - **Covariances**

# Material Balance Evaluation

## Error Models

---

Typical models used in safeguards

- Additive:  $M_i = T + S + R_i$
- Multiplicative:  $M_i = T (1 + S + R_i)$

**$M_i$  is the measured value**  
**T is the true value**  
**S is systematic error, and**  
**R is random error**

# Material Balance Evaluation

## Propagation of Variance (POV)

---

### *Combining Lots of Errors!*

- **Combining errors becomes more complicated when dealing with a material balance or many measured values**
- **POV is the determination of the uncertainty for the material balance – combining many errors**
- **Need the specific equation showing how measured values are combined**

# Material Balance Evaluation

## POV example

---

- **Consider 10 cans of Pu oxide each containing 10kg. We would like to know the uncertainty in the total Pu content.**
- **This might represent one term in a material balance equation.**

# Material Balance Evaluation

## POV example

---

- Measure the plutonium in 10 cans of PuO<sub>2</sub>:

$$M = \sum_{i=1}^{10} W_i C_i \text{ where:}$$

M is the measured total mass of Pu,

$W_i = \text{Gross}_i - \text{Tare}_i$  is the measured weight of PuO<sub>2</sub> in can  $i$ , and

$C_i$  is the measured Pu conc (~ 0.88 if high purity) in can  $i$ .

- How close do we expect M to be to  $M_T$ ?

*( $M_T = \text{true mass of Pu}$ )*

# Material Balance Evaluation POV example

---

- Assume the facility estimates:

|   |                             |           |                    |
|---|-----------------------------|-----------|--------------------|
| W | $0.0015^2 \hat{\sigma}_R^2$ | $0.001^2$ | $\hat{\sigma}_S^2$ |
| C | $0.003^2$                   | $0.001^2$ |                    |

**NOTE: square roots of table values are RSDs.**

# Material Balance Evaluation POV example

---

Estimate  $\sigma_M$

- **Simplify by:**
  - **Assuming “stream averages:”**  
 $W_i=10$  kg,  $C_i=0.88$  for each of the 10 cans
  - **Assume no recalibrations of scale or lab procedure**
  - **Assume error model applies to net weight**

# Material Balance Evaluation

## POV example

---

A simple effective measurement error model:

$$W_i = W_{Ti}(1 + S_W + R_{Wi})$$

$$C_i = C_{Ti}(1 + S_C + R_{Ci})$$

*These are multiplicative error models so the  $\sigma$ s are RSDs.*

Factor the constants W and C out of sum to get:

$$M \cong \sum_{i=1}^{10} W_{Ti} C_{Ti} (1 + S_W + R_{Wi} + S_C + R_{Ci})$$

# Material Balance Evaluation

## POV example

---

$$\sigma_M^2 = (10 * 10 * 0.88)^2 (\sigma_{SW}^2 + \sigma_{SC}^2 + (\sigma_{RW}^2 + \sigma_{RC}^2)/10)$$

$$\sigma_M^2 = 0.24 \text{ kg}^2$$

$$\sigma_M = 0.16 \text{ kg}$$

**(0.18% of total Pu mass of 88 kg)**

# Material Balance Evaluation

---

- To extend POV to the material balance, follow the previous example for all terms in the MB equation
- Consider covariances – now likely
- Result is  $\sigma_{ID}$
- Loss detection
  - Limit of error of ID
    - Applies to an individual material balance
    - Results from measurement uncertainty
  - $ID > 2 * \sigma_{I\Delta}$  is “warning”
  - $ID > 3 * \sigma_{I\Delta}$  is “alarm”

# Material Balance Evaluation

## Complications

---

- **Unmeasured inventory/holdup**
- **Seasonal or other patterns**
- **Item or matrix specific biases (e.g., difficult to measure materials)**
- **Poorly estimated individual errors because performance on real items is worse than on standards**

# Exercise

---

- **Large Group Exercise (tank example for LEID calculation)**



# Lecture 8

---

## Target Analysis



# Learning Objective

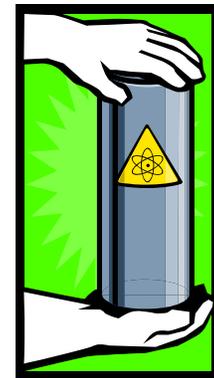
---

- **Understand the basic steps of target identification**
- **Recognize the considerations necessary to establish protection goals**
- **Identify the two basic types of target identification methodologies**

# Targets of Interest

---

- **Identify targets to be evaluated:**
  - **Nuclear materials**
    - **Theft Targets**
      - Discrete items
      - Bulk materials
    - **Strategies**
      - Abrupt Theft
      - Roll-up
      - Protracted Theft
  - **Sabotage Targets**
    - Radiological
  - **Classified information and/or matter**
  - **Others as appropriate**



# Roll Up

---

## What is Roll-Up?

- *The accumulation of smaller quantities of special nuclear material to a higher category*

## Why is Roll-up calculated and Categorized

- *lesser materials are usually treated differently than goal quantities and generally there is greater access*

## Why is it a concern?

- MPC&A Measures may be less restrictive for smaller quantities
  - Physical protection
  - Surveillance measures
  - Access controls
  - Inventories (less frequent, <100% sampled)

## Is it always an issue?

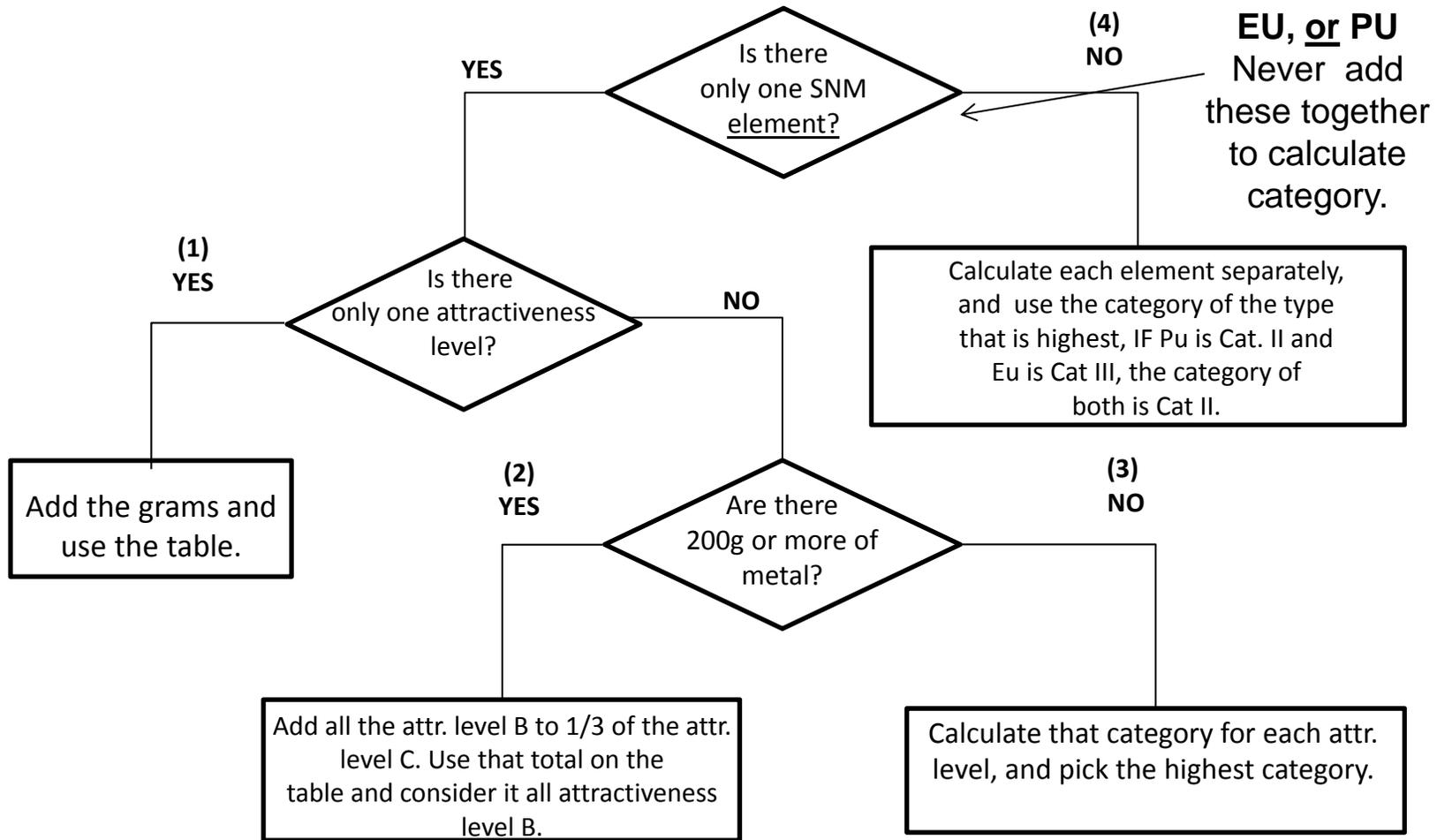
- Credibility of roll up depends on material type, form and likelihood that the Insiders could accumulate a goal quantity before detection

# Is Roll Up Credible?

---

- Materials outside of MAAs
  - Is the total amount of SNM greater than a goal quantity
  - Can the Insiders gain access to enough areas to accumulate a goal quantity at a point in time
  - Can the Insiders credibly accumulate a goal quantity before detection (or with a lower probability of detection)
- Materials within a MAA
  - Are lesser attractive materials treated differently
  - Can Insiders accumulate a goal quantity before detection (or with a lower probability of detection)
  - Can Insiders divert and hide and accumulate the material undetected prior to removal

# Category Calculations (for PU/HEU)



# Protracted Theft or Diversion

---

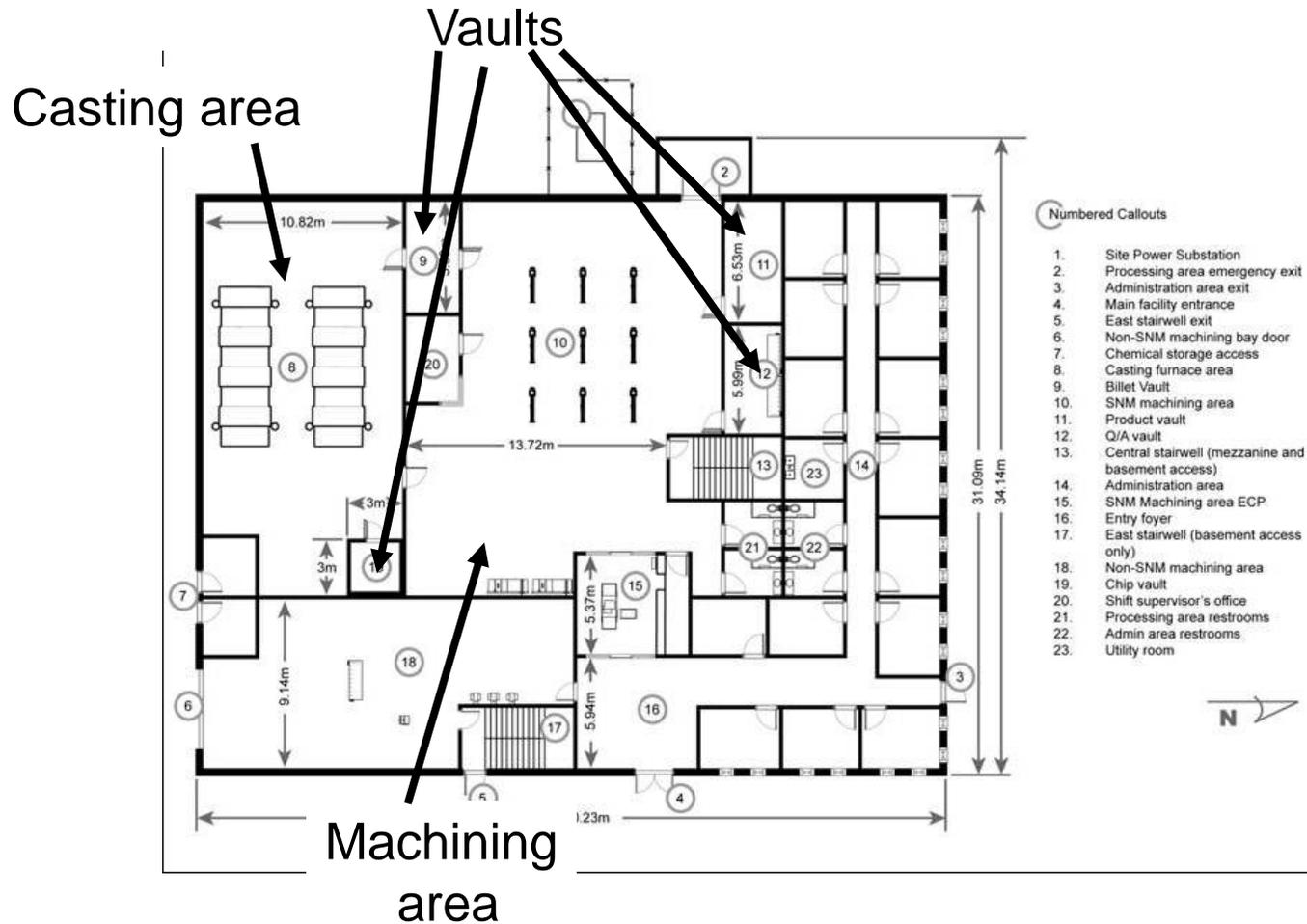
- **Protracted theft from MAA (repeated attempts)**
  - Small quantities – easier to remove undetected
  - Requires multiple theft attempts
  - Longer time line than an abrupt theft
  - Chances of being detected increase as the number of attempts needed increases
  
- **Protracted diversion to unauthorized location - abrupt theft from site**
  - Small quantities – easier to divert undetected
  - Requires multiple diversion attempts
  - Longer time line than an abrupt theft
  - Chances of being detected during accumulation process increases with each diversion attempt
  - Still requires undetected removal from MAA

# Protracted Theft Strategies

---

- **Protracted Theft or Diversion may involve the substitution of material to reduce the probability of being detected**
- **Credible Substitution Materials**
  - Material that can be successfully used in place of accountable special nuclear material. This substitution is possible because of one or more physical properties shared by the substitution material and the special nuclear material.

# Uranium Recovery Facility (URF): Target Identification and Location



# Material on Site at the URF

| Material Balance Area | Form of Material   | Allowable Material Inventory (wt % enrichment) |
|-----------------------|--|--|
| X-Ray Facility        | Uranium Metal – billets  | 5 kg U (>86.6%)                                |
| Product Bunker        | Uranium Metal – billets  | 300 kg U (>86.6%)                              |
|                       | UO <sub>2</sub> – loose powder   | 10 kg U (>86.6%)                               |
| Processing Building   | Uranium Metal – ingots   | 30 kg U (>86.6%)                               |
|                       | UO <sub>2</sub> – loose powder<br>Uranium Metal – scrap<br>or input material (e.g.,<br>chips and turnings) | 50 kg U (>86.6%)                               |
|                       | Uranium Metal – billets  | 20 kg U (>86.6%)                               |
| Analytical Laboratory | Samples all forms  | 3 kg U (>86.6%)                                |

# Areas and Operations in the URF

---

- **Casting Furnace Area** – two furnaces where  $\text{UO}_2$  powder is cast into ingots
- **Billet Vault** – finished ingots stored
- **SNM Machining Area** – nine milling machines process raw ingots to finished billets
- **Product Vault** – stores finished ingots until sent to QA or Storage Bunker
- **QA Vault** – limited number of in-process billet samples and finished ingots
- **Administrative Area (AA)** – general offices
- **Chip Vault** – stores return stream waste from Casting Furnace and Machining Area
- **Analytical Laboratory** – analyzes all Uranium samples
- **X-Ray facility** – diagnostic facility

# Apply Graded Safeguards to Targets on Site

---

- **Provide the greatest protection to material where loss has the highest potential consequence**
- **In this context, potential consequence of loss is generally based on quantity of material and the ease with which the material can be used in making a nuclear device**

# Graded Safeguards Concept Allocates More Security Resources to Higher Value Targets

More attractive



Less attractive

Most Protection



Least Protection

Smallest quantities

Largest quantities

Level of protection is consistent with consequence of loss.

# Target Characteristics - DOE

---

**For each target specify:**

- **Attractiveness level with description**
- **Isotope (Pu,U-233, U-235, Np-237, Am-241, Am-243)**
- **Quantities (mass)**
- **Irradiation Level**
- **Location**
- **Residence time (duration)**
- **Frequency of use or access**

# Categorization of Nuclear Material (U.S. DOE)

|  | Attractiveness Level | Pu/U-233 Category (kg) |        |          |                       | Contained U-235/Separated Np-237/Separated Am-241 and -243 Category (kg) |       |            |                       | All E Materials Category IV |
|--|----------------------|------------------------|--------|----------|-----------------------|--|-------|------------|-----------------------|-----------------------------|
|  |                      | I                      | II     | III      | IV                    | I  | II    | III        | IV                    |                             |
| <b>WEAPONS</b><br>Assembled weapons and test devices   | A                    | All                    | N/A    | N/A      | N/A                   | All  | N/A   | N/A        | N/A                   | N/A                         |
| <b>PURE PRODUCTS</b><br>Pits, major components, button ingots, recastable metal, directly convertible materials  | B                    | >2                     | >0.4<2 | >0.2<0.4 | <0.2                  | >5   | >1<5  | >0.4<<br>1 | <0.4                  | N/A                         |
| <b>HIGH-GRADE MATERIALS</b><br>Carbides, oxides, nitrates, solutions (>25 g/L) etc.; fuel elements and assemblies; alloys and mixtures; UF <sub>4</sub> or UF <sub>6</sub> (> 50% enriched)                                | C                    | >6                     | >2<6   | >0.4<2   | <0.4                  | >20  | >6<20 | >2<6       | <2                    | N/A                         |
| <b>LOW-GRADE MATERIALS</b><br>Solutions (1 to 25 g/L), process residues requiring extensive reprocessing; moderately irradiated material; Pu-238 (except waste); UF <sub>4</sub> or UF <sub>6</sub> (> 20% < 50% enriched) | D                    | N/A                    | >16    | >3<16    | <3                    | N/A  | >50   | >8<50      | <8                    | N/A                         |
| <b>ALL OTHER MATERIALS</b><br>Highly irradiated forms, solutions (<1 g/L), uranium containing <20% U-235 or <10% U-2332 (any form, any quantity)   | E                    | N/A                    | N/A    | N/A      | Reportable Quantities | N/A  | N/A   | N/A        | Reportable Quantities | Reportable Quantities       |

# Example Consequence Table Based on Material Form and Categories

| Form          | Category I | Category II | Category III |
|---------------|------------|-------------|--------------|
| Weapons       | 1.0        | N/A         | N/A          |
| Pure products | 0.5        | 0.25        | 0.1          |
| High grade    | 0.25       | 0.1         | 0.05         |
| Low grade     | 0.1        | 0.05        | 0.02         |
| Other         | 0.05       | 0.02        | 0.01         |

Example: Consequence of theft of a 2 kg HEU metal button (Pure Product, Category II) is 0.25.

Actual table would be determined by government policy.

# Summary

---

- **Target identification must begin with definition of the risks or consequences of what is to be protected against.**
- **Target identification based on both physical form and quantity.**
- **The output of the target identification process is referential information (target characteristics and location) tied to consequence levels (target importance).**



## Lecture 9

---

# Insider Characterization Identify Potential Insiders



# Learning Objective

---

- **Gather information on potential insiders based on job functions**
- **Generate threat group tables for targets**

# Gather Facility-specific Information about Potential Threat

---

- **Facility conditions**
  - Employee morale
  - Operations going well?
  - Union disagreements
  - Organization / security culture
- **Conditions outside the facility**
  - Community approval of facility
  - Activists in the community
- **Facility features**
  - Operating conditions at all times
  - Built-in protection features and weaknesses



# Collect Potential Insider Information

- **Identify general personnel assignments**
- **Ensure that all assignments to critical areas are included**
- **Identify unique groups that could be responsible for theft or sabotage**
- **Understand each work group's potential capabilities**



# Guidelines and Methods for Grouping

---

- **Personnel should be grouped whenever:**
  - **Types have identical access, authority, knowledge and capability**
  - **Access, authority, and knowledge of one type is completely a subset of another**
  - **Access, authority, and knowledge are nearly identical**
    - **Create a composite group to cover both (be conservative)**
- **Groups may be target-dependent**
- **Two methods for grouping**
  - **Expert judgment**
  - **Data based**

# Two Methods for Grouping

---

## 1. Expert judgment grouping

- Preliminary grouping
- Limited site access
- Incomplete data

## 2. Data based grouping

- Job descriptions
- Site access data
- Personnel discussions / interviews



# Attributes to Consider during Grouping

---

- **Access**
- **Authority**
- **Knowledge**



# Potential Insider ACCESS Attribute Considerations

---

- Limited areas
- Protected areas
- Vital areas
- Nuclear materials
- CAS
- Alarms
- Keys
- Badging
- Information management of access system
- NM records
- NM forms
- Site vehicles
- Tools
- Controlled information



# Potential Insider **AUTHORITY** Attribute Considerations

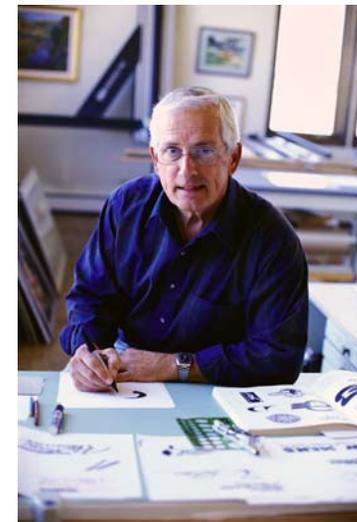
---

- **Supervisory**
- **Supervisory over guards**
- **Personal vehicle**
- **Exempt searches**
- **Exempt metal detector**
- **Exempt NM detector**
- **Authorize NM transfers**
- **Prepare NM transfers**
- **Verify NM transfers**
- **Verify inventory**
- **Assess alarms**
- **Issue badges**
- **Issue access codes**
- **Prepare access lists**
- **Equipment maintenance**

# Potential Insider KNOWLEDGE Attribute Considerations

---

- Procedures
- Processes
- Target Locations
- Site details
- MPC&A System details
- Guard postings
- Response Plans
- Frequency of events
- Potential vulnerabilities
- Tools and equipment
- Procedure violations



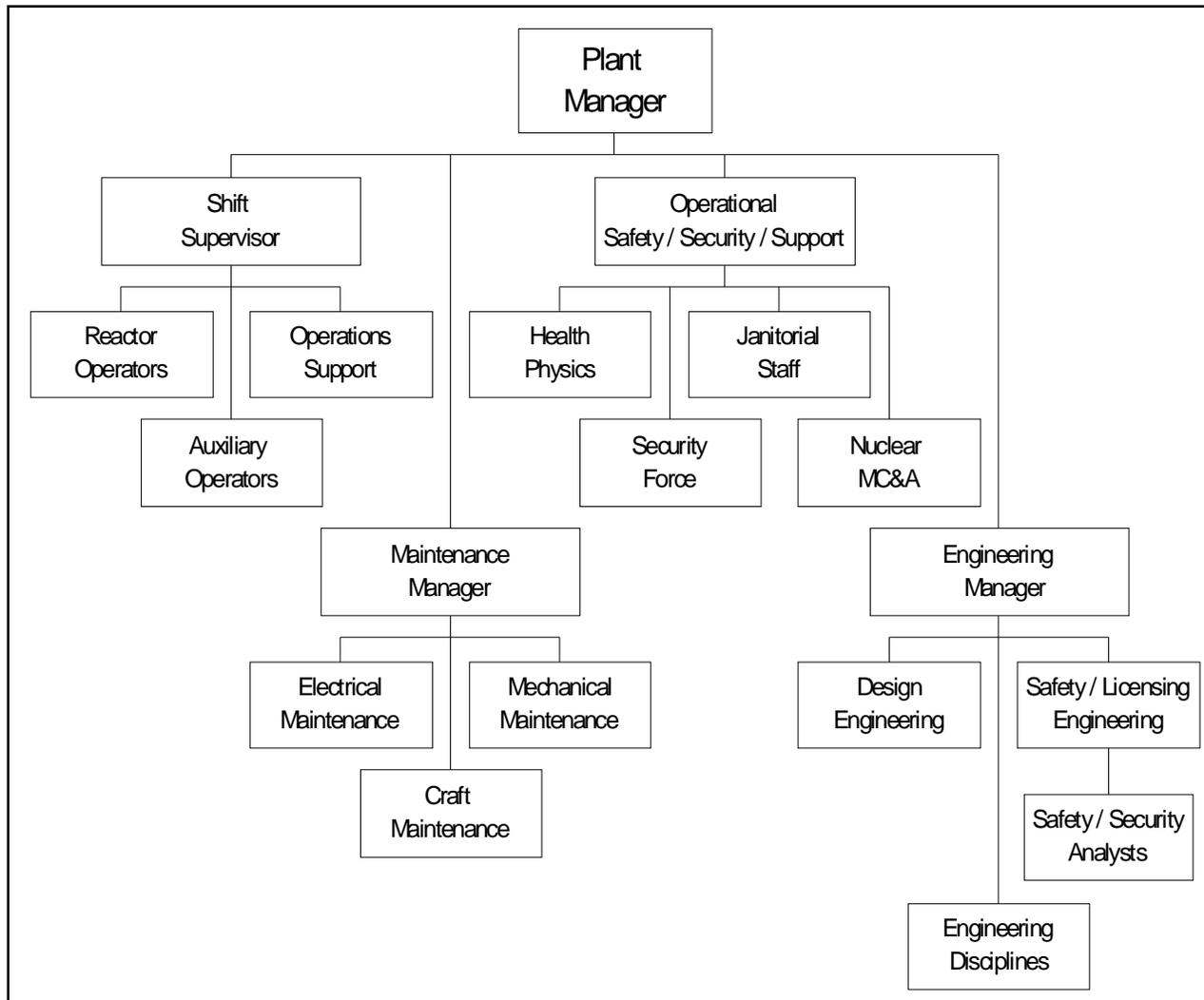
# Develop Insider Groups – Method 1 (Expert Judgment Grouping)

---

- 1. Review site documentation**
  - Review organizational information and job descriptions
- 2. Examine organization chart**
  - Group common job functions
- 3. Identify possible persons not on organization chart**
  - Examine site and targets access lists
- 4. Interview representatives from each group to determine insider overall capability for each target**
  - Access
  - Authority
  - Knowledge



# Examine Organization Chart



- Inspectors?
- Vendors?
- Official visitors?
- Contractors?
- Public visitors?
- Emergency personnel?

# Personnel Types

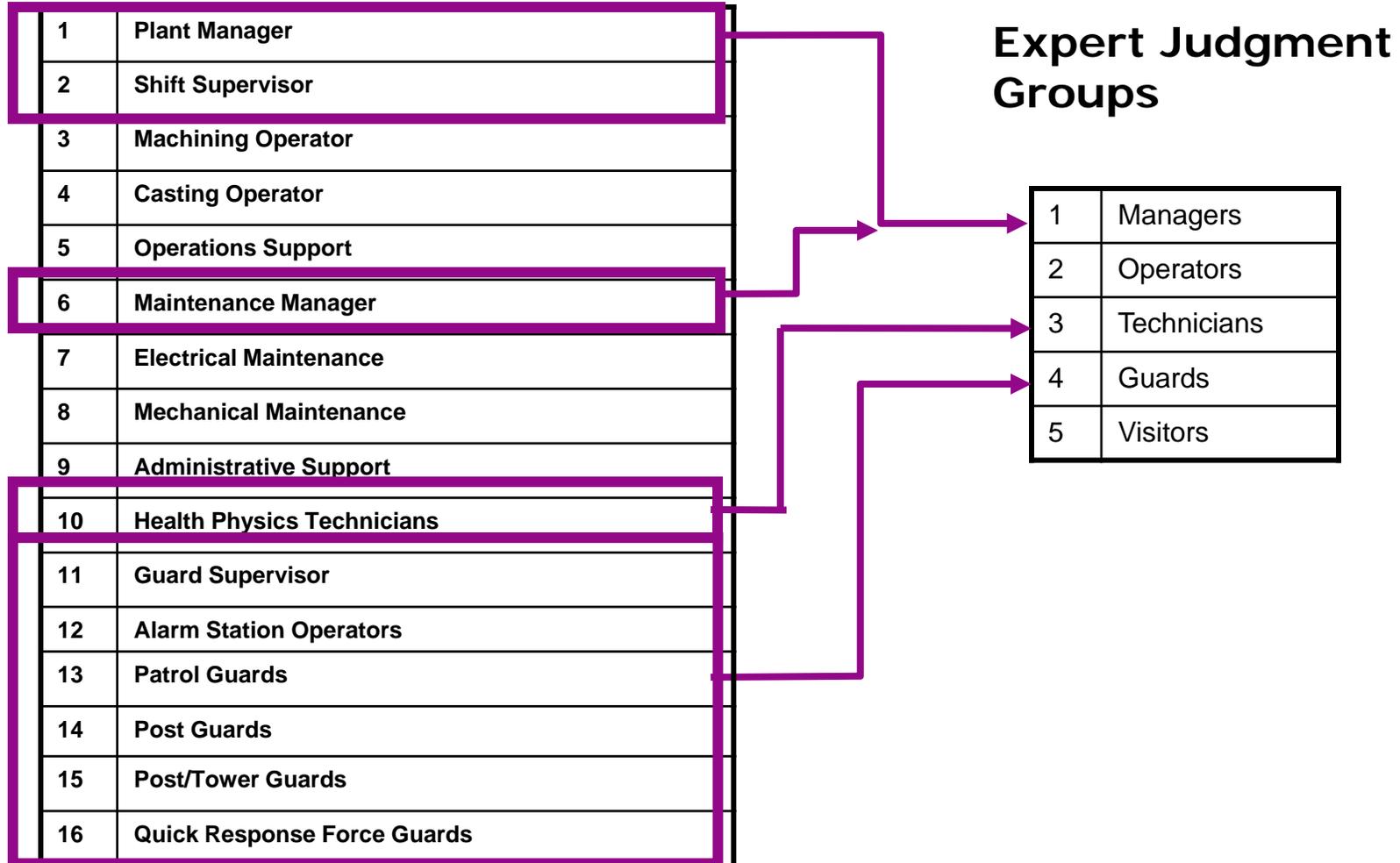
|    |                             |
|----|-----------------------------|
| 1  | Plant Manager               |
| 2  | Shift Supervisor            |
| 3  | Machining Operator          |
| 4  | Casting Operator            |
| 5  | Operations Support          |
| 6  | Maintenance Manager         |
| 7  | Electrical Maintenance      |
| 8  | Mechanical Maintenance      |
| 9  | Crafts Maintenance          |
| 10 | Administrative Support      |
| 11 | Health Physics Technicians  |
| 12 | Guard Supervisor            |
| 13 | Alarm Station Operators     |
| 14 | Patrol Guards               |
| 15 | Post/Tower Guards           |
| 16 | Quick Response Force Guards |

|    |   |
|----|---|
| 17 | Janitorial Staff  |
| 18 | Material Balance Area Custodians                                      |
| 19 | Nuclear Material Technicians  |
| 20 | Nuclear Material Accountability Technicians                           |
| 21 | Engineering Support   |
| 22 | Design, Mechanical, Electrical, Civil, Chemical and Nuclear Engineers |
| 23 | Safety Engineers  |
| 24 | Security Analysts   |

## Non-Employee Access to URF

|    |                                  |
|----|----------------------------------|
| 25 | Vendors                          |
| 26 | State Safety/Security Inspectors |

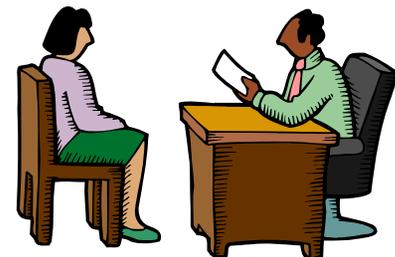
# Expert Judgment Attribute Grouping Example



# Develop Insider Groups – Method 2 (Data Based Grouping)

---

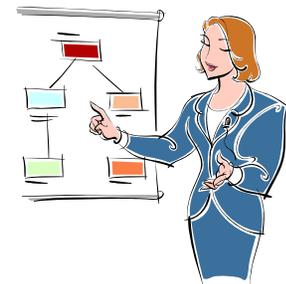
- 1. Review site documentation including organization chart**
  - Review organizational information and job descriptions
  - Examine site and targets access lists
- 2. Generate a comprehensive list of personnel with access by job function**
- 3. Interview representatives from each job function to determine insider characteristics for each target**
  - Access
  - Authority
  - Knowledge



# Develop Insider Groups – Method 2 (Data Based Grouping) *(cont'd)*

---

- 4. Group job functions by access, authority, and knowledge attributes**
- 5. Prioritize job function groups for analysis based on attribute evaluation**



# Interview Representatives

---

- **Interviews are essential to gain unknown information**
- **Mutual cooperation is essential for success**
- **Results must be attributed to personnel types**
- **An unbiased professional approach is necessary**
- **Be prepared and as knowledgeable as possible**
- **Ensure that the person understands the purpose of the interview**
- **Generate an environment of comfort for the person**
- **Ask probing questions that require an explanation**
- **Do not argue or take personal offense**
- **Take notes, thank the person, and summarize**

# Suggestions for Qualitative Designators (H, M, L)

| Attribute         | High   | Medium  | Low  |
|-------------------|--|---|--|
| <b>Access</b>     | Authorized at all times normally on site – Target always available   | Authorized on specific occasions – Limited target availability  | No authorization   |
| <b>Authority</b>  | Almost anything commanded is done without question   | Has limited or temporary authority or considerable personal influence   | Little authority   |
| <b>Knowledge*</b> | Details of operations and systems. Has the equipment, tools, and skills to accomplish the malevolent acts. | General understanding of operations and systems or detailed knowledge of limited areas. Might have some of the equipment, tools and skills to accomplish the malevolent acts. | Little understanding. Does not have the equipment, tools and skills to accomplish the malevolent acts. |

*\* Assume only the knowledge and capability required to conduct assigned responsibilities*

# Example Form for Collecting / Recording Data

---

**Job Type** \_\_\_\_\_ **Date** \_\_\_\_\_

| <i>Target</i> | <i>Level of Access</i> | <i>Level of Authority</i> | <i>Level of Knowledge</i> | <i>Notes</i> |
|---------------|------------------------|---------------------------|---------------------------|--------------|
|               |                        |                           |                           |              |
|               |                        |                           |                           |              |
|               |                        |                           |                           |              |
|               |                        |                           |                           |              |

# Example Form for Collecting / Recording Data

**Job Type:** Health Physics

**Date:** 12 Nov 06

| Target               | Level of Access | Level of Authority | Level of Knowledge | Notes   |
|----------------------|-----------------|--------------------|--------------------|---|
| <i>Bunker</i>        | <i>M</i>        | <i>L</i>           | <i>L</i>           | <i>MBA Custodian controls vault - escorts</i> |
| <i>Casting Area</i>  | <i>H</i>        | <i>L</i>           | <i>L</i>           |   |
| <i>Product Vault</i> | <i>M</i>        | <i>L</i>           | <i>L</i>           | <i>MBA Custodian controls vault - escorts</i> |
| <i>Billet Vault</i>  | <i>M</i>        | <i>L</i>           | <i>L</i>           | <i>MBA Custodian controls vault - escorts</i> |

# Learning Objectives

---

- **Gather information on potential insiders based on job functions**
- **Generate threat group tables for targets**

# Threat Group Tables

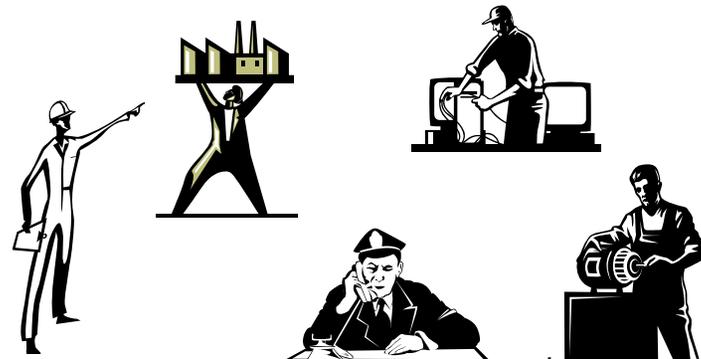
---

- **Develop characteristics of insider groups**
- **Generate a list of groups at the facility**
- **Define qualitatively (High, Medium, or Low) the level of access, authority, and knowledge that each insider group has for each target**

*The lists for different targets will be very similar but the differences are important as we conduct the analysis*

# Example for Developing Threat Group Tables

- Use the descriptors in slide 21 “Suggestions for Qualitative Designators”
- Apply the H, M, L rules for each characteristic
  - Access
  - Authority
  - Knowledge
- As an example, create a threat group table for:
  - Five job positions
  - Bunker targets



# Example of H,M,L Applied to Threat Group Table for the Bunker

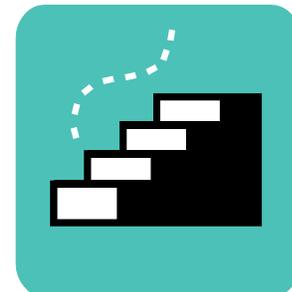
| Position (Number)  | Routine Access   | Routine Authority / Responsibility  | Knowledge  |
|--|--|---|--|
| Plant Manager (1)<br>(Plant Manager Org.)  | Protected Area, All Inner Areas (usually escorted) <b>L</b>                        | Overall direction. Not authorized to direct detailed facility operations <b>M</b>                             | General knowledge of plant operations, lacks detailed understanding of facility <b>M</b>               |
| Shift Supervisor (3 total with 1 per shift)<br>(Shift Supervisor Org.)                     | Protected Area, All Inner Areas <b>L</b>   | Detailed direction of all facility activities. Directions obeyed without question in most situations <b>H</b> | Extensive, detailed knowledge about all aspects of facility design, layout, and operation. <b>M</b>    |
| Machining operator (6 total with nominal 4 per day shift)<br>(Operations Support Org.)     | Protected Area, All Inner Areas <b>L</b>   | Detailed direction of all machining activities. Under direction of shift supervisor. <b>L</b>                 | Extensive, detailed knowledge about all activities in the machining area. <b>M</b>                     |
| Health Physics Technicians (4 total with nominal 3 per day shift)<br>(Health Physics Org.) | Protected Area, all Inner Areas and occasional escorted access to Storage <b>M</b> | Monitor radiological conditions. Not permitted to work on plant equipment. <b>L</b>                           | Specialized knowledge related to their duties. Narrow knowledge of facility systems. <b>M</b>          |
| Operations Support (6 total with nominal 4 per day shift)<br>(Operations Support Org.)     | Protected Area, All Inner Areas and occasional escorted access to Storage <b>M</b> | Perform specific operations tasks under direction of machining and casting operators <b>L</b>                 | Specialized knowledge related to their duties. Narrow knowledge of complete facility systems. <b>M</b> |

# Partial Position Listing for the Bunker

| <b>Job Position</b>               | <b>Access</b> | <b>Authority</b> | <b>Knowledge</b> |
|-----------------------------------|---------------|------------------|------------------|
| <b>Plant Manager</b>              | <i>L</i>      | <i>M</i>         | <i>M</i>         |
| <b>Shift Supervisor</b>           | <i>L</i>      | <i>H</i>         | <i>M</i>         |
| <b>Machining Operator</b>         | <i>L</i>      | <i>L</i>         | <i>M</i>         |
| <b>Health Physics Technician</b>  | <i>M</i>      | <i>L</i>         | <i>M</i>         |
| <b>Operations Support</b>         | <i>M</i>      | <i>L</i>         | <i>M</i>         |
| <b>Maintenance Manager</b>        |               |                  |                  |
| <b>Mechanical Maintenance</b>     |               |                  |                  |
| <b>Health Physics Technicians</b> |               |                  |                  |
| <b>Alarm Station Operators</b>    |               |                  |                  |
| <b>Post Guards</b>                |               |                  |                  |

# Bunker Example - Prioritize Insider Groups

- Preliminarily rank the five positions for the bunker using the following rules:
  - Utilize the access characteristic first and select those groups with the highest level of access
  - For groups with equally high access, utilize the authority characteristics of these groups to differentiate
  - Use the knowledge characteristics as needed for additional differentiation



# Highest Degree of Access for the Bunker Targets

| Position                  | Routine Access | Routine Authority / Responsibility | Knowledge |
|---------------------------|----------------|------------------------------------|-----------|
| Health Physics Technician | <i>M</i>       | <i>L</i>                           | <i>M</i>  |
| Operations support        | <i>M</i>       | <i>L</i>                           | <i>M</i>  |

# Next Highest Degree of Access for the Bunker Targets

| Position (Number)  | Routine Access | Routine Authority / Responsibility | Knowledge |
|--------------------|----------------|------------------------------------|-----------|
| Shift Supervisor   | <i>L</i>       | <i>H</i>                           | <i>M</i>  |
| Plant Manager      | <i>L</i>       | <i>M</i>                           | <i>M</i>  |
| Machining Operator | <i>L</i>       | <i>L</i>                           | <i>M</i>  |

*Continue the process for all the insider positions*

# Insider Threat Characterization Summary

---

- **We now have:**
  - **A definition of targets that we will be applying the threat against**
  - **Ranked positions of specific potential insider groups at the facility**
    - **They have been generated considering access, authority, and knowledge**

# Module Summary

---

- Review the insider threat basic concepts
- List the three major insider attributes
- Recognize the role of the National DBT
- Characterize the insider portion of the DBT for the facility
- Gather information on potential insiders based on job functions
- Generate threat group tables for targets

Questions or Comments?



# Sub-Group Exercise: Prioritize the Insider Threat

---

- **Use the URF personnel tables from the exercise materials in this module – identify job positions**
- **Create threat group table with descriptor for each insider attribute (access, authority, knowledge)**
- **Assign qualitative designators (H, M, L) to each job position for the same theft targets you used in your target sub-group exercise:**
  - **The X-ray facility during day shift**
  - **The processing building**
    - **The product vault during night shift**
    - **The machining area during day shift**
    - **The chip vault during night shift**

# Sub-Group Exercise: Prioritize the Insider Threat *(cont'd)*

---

- **Select the five “highest insider threat” positions for each target**
- **Present your results for a large group discussion**
  - **We will use these as the insider threat groups for the rest of the overview course**



# Lecture 10

---

## Case Studies



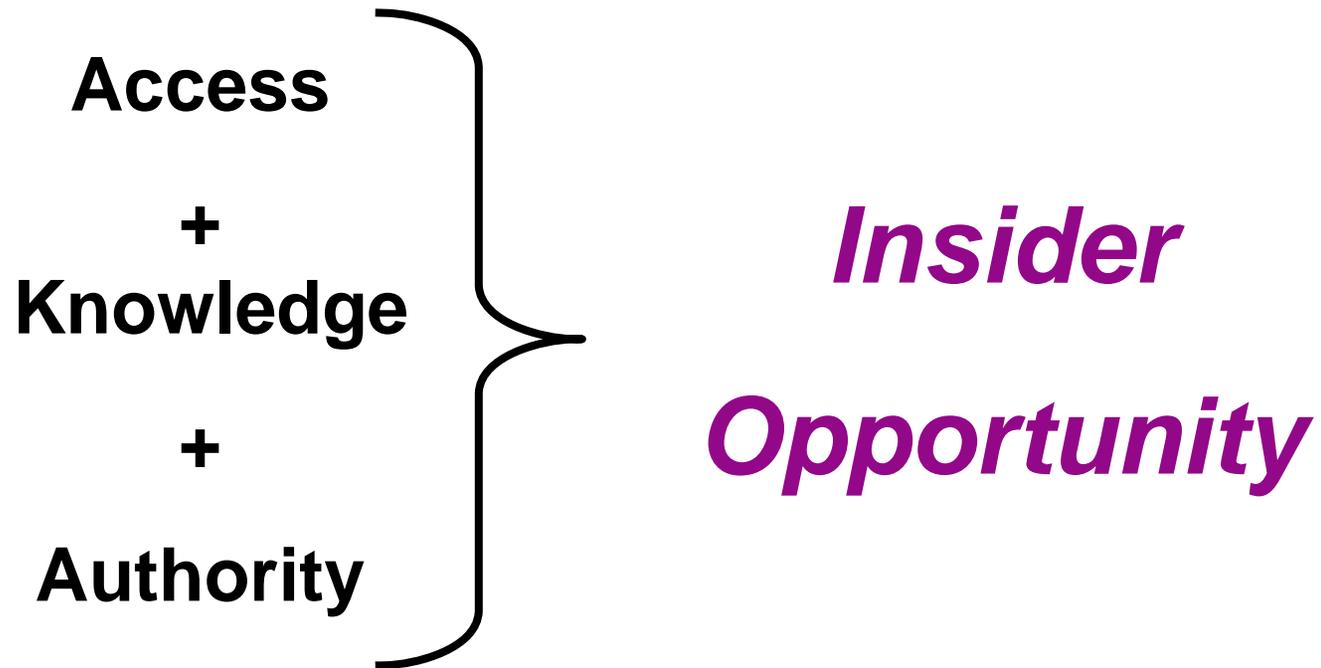
# Learning Objective

---

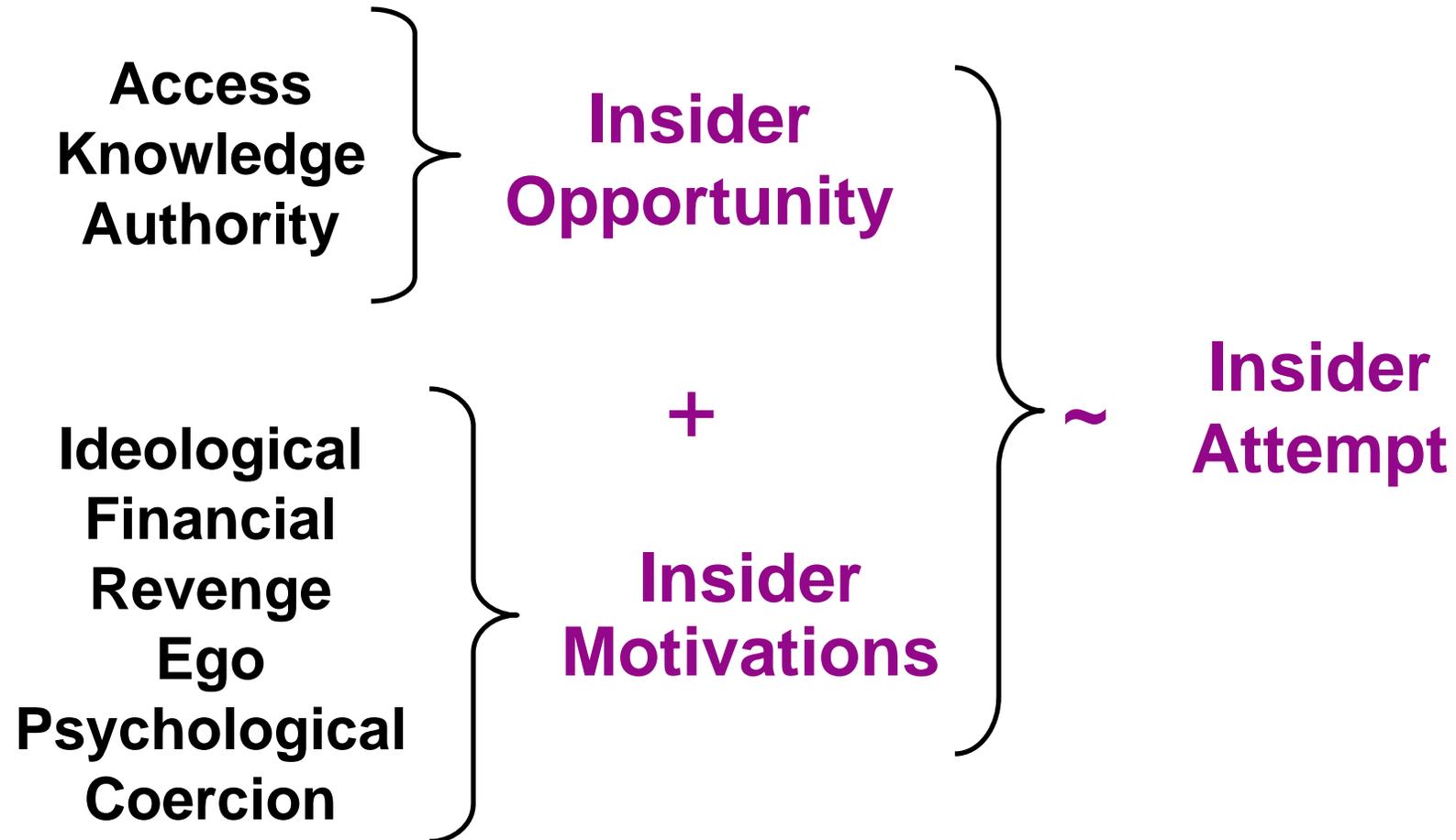
- **Gain better appreciation of insider motivations**
- **Become familiar with some real examples of insider actions**

# Opportunity

---



# Factors Affecting Unauthorized Insider Actions



# Malevolent Insider Examples

---

- **Case Study Exercise**



# Lecture 11

---

## Insider Analysis - Sequence of Actions



# Learning Objective

---

- **VA working group composition**
- **VA limitations and assumptions**
- **Briefly review methodologies to evaluate protection systems**
- **Apply the methodology to produce a sequence of insider threat actions**
- **Identify existing measures that protect targets against threat actions**

# Establish a Vulnerability Analysis Working Group

---

## VA Core Team Members

- Vulnerability Analysis
- MC&A Custodian
- Facility physical protection
- Facility operations
- Performance testing
- Protective force

## VA Team Selection Criteria

- Experience Required
- Team Diversity

## VA Support Team Members

- Facility manager
- PP maintenance
- MC&A measurements
- Nuclear material handler
- Shipments
- Waste stream
- Safety
- Criticality
- Other Managers and Experts as needed

# Limitations/Assumptions

---

- **Analysis addresses detection and assessment of a single non-violent insider using abrupt or protracted theft**
- **Detection after the action has been completed is considered in recovery and mitigation actions**
- **Analysis of insider in collusion with an outsider threat is NOT included in course**
- **Industrial or radiological sabotage not addressed in course**
- **Other limitations/assumptions as necessary to “focus” the analysis**



# Select a Threat Group/Target Combination

---

- Select the highest priority targets first
- Select the highest threat insider group(s) for each specific target as a starting point
- All the insider threat groups and target combinations need to be evaluated. Many of the details developed for the higher threat groups will also be applicable to the lower threat groups.
  - (Number of targets) x (Number of insiders) x (number of scenarios) = big number?
  - URF has 25 worker types!

# Evaluation Methodologies – Graded Approach

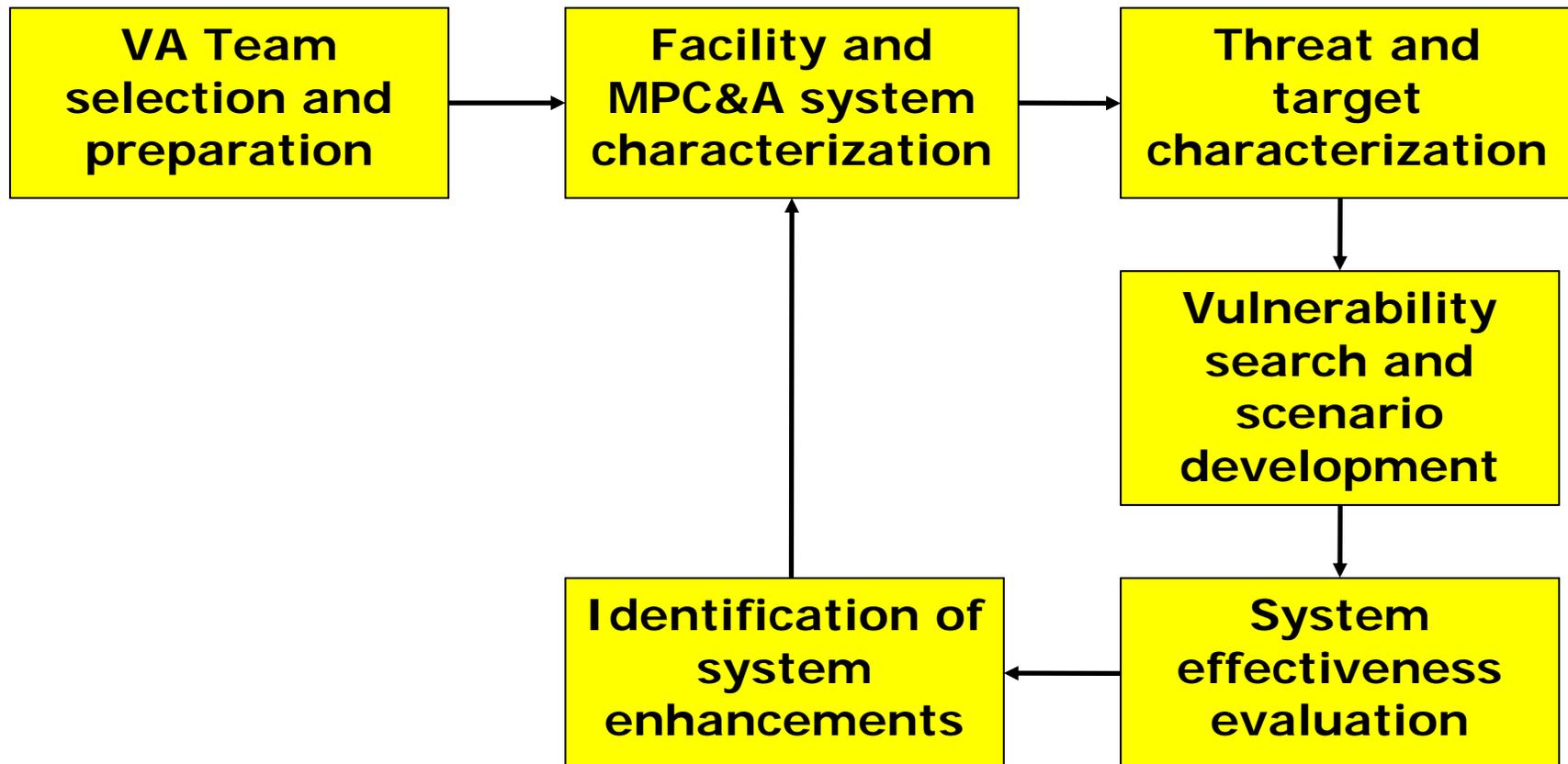
---

## Simple verses complex methods

- Simple facility or low consequence target
  - Expert opinion (Subject Matter Experts – SMEs)
  - Simple analysis (Checklist methods)
  - Performance testing and validation
- Moderately complex facility or moderate consequence target
  - Expert opinion
  - Manual scenario generation and analysis (e.g. VISA)
  - Performance testing and validation
- Highly complex facility or high consequence target, all of above plus:
  - Automated scenario generation and analysis (e.g. ASSESS)
  - Simulations

We will illustrate the VA process manually.

# Vulnerability Assessment Steps



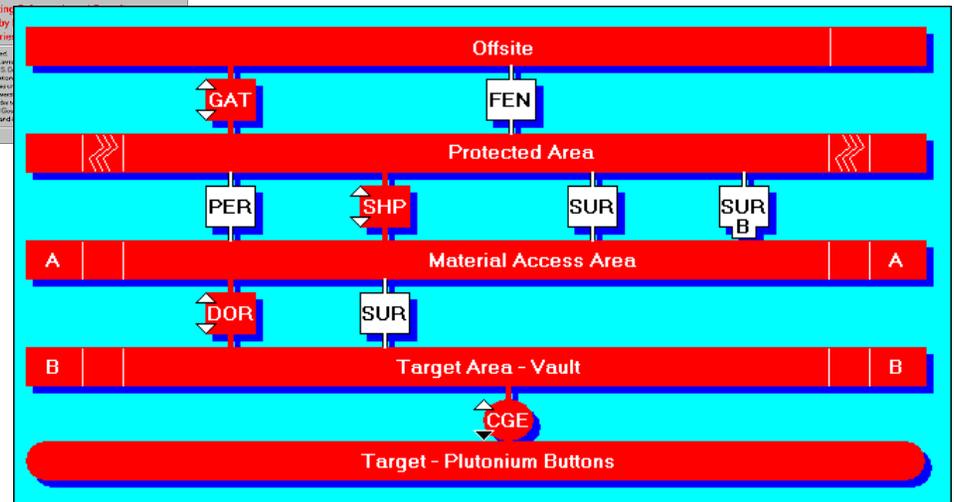
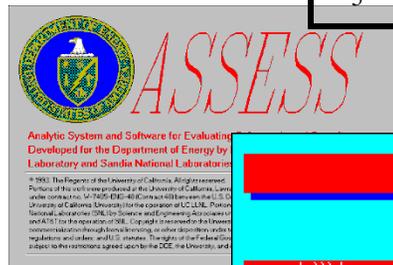
# Methodologies for Evaluating Insider Protections Systems

## Checklist

- **Safeguards**
  - Access Controls
  - Contraband Detection
  - SNM Detector
  - Intrusion Detection
  - Access Delay
  - Security Inspectors
- **Material Accounting**
  - Accounting Systems
  - Physical inventories
  - Measurement and measurement controls
  - NM transfers
  - Material control indicators
- **Material Control**
  - Access controls
  - Material surveillance
  - Material containment
- **Detection and assessment**

G-TAP

| Vulnerability of Integrated Security Analysis (VISA) |                  |      |      |      |      |            |
|--|------------------|------|------|------|------|------------|
| Step No.   | Step Description | P(D) | P(A) | P(I) | P(N) | Step Score |
| 1  | Enter Perimeter  | M    | H    | M    | M    | M          |
| 2  | Enter Bunker     | L    | M    | M    | M    | L          |
| 3  | Acquire Material | H    | L    | M    | M    | L          |
| 4  | Exit Bunker      | H    | H    | M    | L    | L          |
| 5  | Exit Perimeter   | H    | H    | L    | L    | L          |
| System Effectiveness (SE):                           |                  |      |      |      |      | M          |



Analytical System and Software for Evaluation Safeguards and Security

# Methodology for Evaluating the Protection System

---

1. Develop a sequence of adversary actions for each target



2. Identify measures that protect against these actions



3. Characterize protection measures



4. Develop vulnerable paths



5. Develop worst case scenarios

# Develop a General Sequence of Actions

---

- Describe the general actions that need to be accomplished
- Identify the areas to be crossed by the insider
- Identify the actions needed to accomplish the insider goal



# Example: Develop a General Sequence of Actions for Theft Target

Threat – Nuclear Material Technician (NMT)

Target – Recycle material on open shelves in Bunker

| Step | Area          | Insider Actions           |
|------|---------------|---------------------------|
| 1    | Enter PA      | Authorized access         |
| 2    | Enter Bunker  | Authorized access         |
| 3    | Inside Bunker | Acquire Target            |
| 4    | Bunker        | Remove Target from bunker |
| 5    | PA            | Remove target from PA     |

# Identify Strategies to Accomplish Each Action

---

- **Describe insider strategies to accomplish each of the actions**
  - **Ways to acquire the target**
  - **Ways to move a target from one location to another**
- **Include a broad range of strategy alternatives that might be effective against a broad range of protection elements**
- **May involve stealth or deceit**

# Example: Strategies to Accomplish Each Action

Threat – Nuclear Material Technician (NMT)

Target – Recycle material on open shelves in Bunker

| Step | Area          | Insider Actions           | Insider Strategies             |
|------|---------------|---------------------------|--------------------------------|
| 3    | Inside Bunker | Acquire Target            | Hide on person                 |
|      |               |                           | Falsify shipment               |
| 4    | Bunker        | Remove target from Bunker | Hide on person                 |
|      |               |                           | Hide with tools or equipment   |
|      |               |                           | Falsify shipment               |
| 5    | PA            | Remove target from PA     | Hide on person                 |
|      |               |                           | Hide with tools or equipment   |
|      |               |                           | Hide with waste                |
|      |               |                           | Hide in vehicle with shielding |
|      |               |                           | Throw over fence               |

(Steps 1 and 2 omitted because NMT has authorized access.)

# Methodology for Evaluating the Protection System

---

1. Develop a sequence of adversary actions for each target



2. Identify measures that protect against these actions



3. Characterize protection measures



4. Develop vulnerable paths

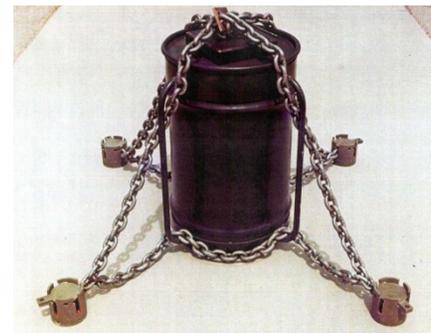


5. Develop worst case scenarios

# Identify Protection Measures Along Action Sequence (Base Case)

---

- 1. Identify all existing protection measures that may prevent, detect, or delay the insider actions**
  - Identify technological measures that may detect or delay the adversarial actions
  - Identify procedural or administrative measures that may detect or delay the insider actions
- 2. Include every protection measure the insider may encounter as they progresses through the sequence**



# Example: Identify Protection Measures for Each Strategy

| Step | Area          | Actions                   | Insider Strategies             | Existing Protection Measures                               |
|------|---------------|---------------------------|--------------------------------|--|
| 3    | Inside Bunker | Acquire Target            | Hide on person                 | Second NMT in TPR  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      |
| 4    | Bunker        | Remove target from Bunker | Hide on person                 | Second NMT in TPR  |
|      |               |                           | Hide with tools or equipment   | Second NMT in TPR  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      |
| 5    | PA            | Remove target from PA     | Hide on person                 | SNM and Metal Portals, Hand search                         |
|      |               |                           | Hide with tools or equipment   | SNM portal, X-ray, Hand search                             |
|      |               |                           | Hide in vehicle with shielding | Contamination and SNM check, Hand search                   |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      |
|      |               |                           | Throw over fence               | CCTV, General observation, Random patrols, 20 m clear zone |

NMT = Nuclear Material Technician

TPR = Two Person Rule

# Sequence of Actions and Measures to Protect Target

---

- In evaluating a system against an insider threat:
  - The first step is to identify the sequence of insider actions and strategies
  - The second step is to identify existing measures that protect against these actions
    - Both administrative and technical measures



# Module Summary

---

- **Discussed VA working group composition**
- **Discussed the purpose of VA limitations and assumptions**
- **Briefly reviewed methodologies for evaluating the protection system**
- **Applied a methodology to produce a sequence of insider threat actions and strategies**
- **Identified existing measures to protect the targets against insider threat actions**



# Lecture 12

---

## Abrupt Theft Analysis



# Learning Objective

---

- **Review the steps to estimate the effectiveness of each protective measure**
- **Apply this methodology to characterize the protective measures at the URF**
- **Establish likelihood of detection and assessment for each step**
- **Identify most vulnerable protection measures**
- **Develop most vulnerable paths for threat/target combination**

# Methodology for Evaluating the Protection System

---

1. Develop a sequence of adversary actions for each target



2. Identify measures that protect against these actions



3. Characterize protection measures



4. Develop vulnerable paths



5. Develop worst case scenarios

# Estimate The Effectiveness Of Each Measure

---

- 1. Define the possible methods and resources used by the insider to minimize the probability of detection and assessment at each protection measure**
- 2. Identify the probability of detection and assessment likelihood of each protection measure in defeating the insider**

# Defining the Methods

---

- **Use normal authorized actions as far as possible along the path**
- **Detection can only occur with deviation from routine activity**
- **When the insider does deviate from routine, they will try to minimize detection (and if active “violent” insider, will overtly act to minimize delay)**
- **The analyst selects these paths based on the data available and expert opinion**



# Method Used By The Nuclear Material Technician - Theft of Recycle Material from Bunker

| Step | Area          | Actions                   | Insider Strategies             | Existing Protection Measures                               |
|------|---------------|---------------------------|--------------------------------|--|
| 3    | Inside Bunker | Acquire Target            | Hide on person                 | Second NMT in TPR  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      |
| 4    | Bunker        | Remove target from Bunker | Hide on person                 | Second NMT in TPR  |
|      |               |                           | Hide with tools or equipment   | Second NMT in TPR  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      |
| 5    | PA            | Remove target from PA     | Hide on person                 | SNM and Metal Portals, Hand search                         |
|      |               |                           | Hide with tools or equipment   | SNM portal, X-ray, Hand search                             |
|      |               |                           | Hide in vehicle with shielding | Contamination and SNM check, Hand search                   |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      |
|      |               |                           | Throw over fence               | CCTV, General observation, Random patrols, 20 m clear zone |

NMT = Nuclear Material Technician

TPR = Two Person Rule

# Estimate The Effectiveness of Each Measure

---

- 1. Define the possible methods and resources used by the insider to minimize the probability of detection and assessment at each protection measure**
- 2. Identify the probability of detection and assessment likelihood of each protection measure in defeating the insider**

# Likelihood Of Detection And Assessment Guidelines

---

- **“Detection” is the probability an insider activity will be detected by the existing protection measures.**
  - **When the action is perceived by others as a normal activity, detection likelihood is “low”**
- **“Assessment” is the act of correctly assessing the detected insider action as an unauthorized activity**
- **Use quantitative data where possible**
- **Use information about the specific facility AND your expert judgment**
- **In many cases the best approach is to use relative qualitative likelihood in the beginning of an analysis since data often do not exist for many insider detection mechanisms**
  - **Document rationale for decisions**



# Estimate The Effectiveness Of Each Protection Measure

---

- Identify the likelihood of detection and assessment of each measure in defeating the insider action
- *High, Medium* and *Low* qualitative scale used for illustration (used in VISA method)
- Probabilities would be used in automated methods (used in ASSESS)
  - Existing database of default values
  - User override



# Suggested Guidance for Estimating Effectiveness of Measures

| <b>Effectiveness</b> | <b>Weaknesses</b>  | <b>Defeat methods</b>   |
|----------------------|--|---|
| <b>High (H)</b>      | <p>Very difficult to determine the weakness</p> <p>Cannot significantly compromise the measure</p> | <p>Nearly impossible to accomplish because of complexity and unavailability of necessary equipment</p> <p>High likelihood of being detected</p> |
| <b>Medium (M)</b>    | <p>Effort required to determine the weakness</p> <p>Cannot completely compromise the measure</p>   | <p>Difficult to accomplish because of complexity or need for difficult to obtain equipment</p> <p>Medium likelihood of being detected</p>       |
| <b>Low (L)</b>       | <p>Obvious weakness</p> <p>Can completely compromise the measure</p>                               | <p>Easily accomplished without training or equipment</p> <p>Low likelihood of being detected</p>  |

# Estimate Probabilities of Detection (Pd) and Assessment (Pa) of Each Protection Measure

| Step | Area          | Actions                   | Insider Strategies             | Existing Protection Measures                               | Pd | Pa |
|------|---------------|---------------------------|--------------------------------|--|----|----|
| 3    | Inside Bunker | Acquire Target            | Hide on person                 | Second NMT in TPR  | L  | H  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      | M  | M  |
| 4    | Bunker        | Remove target from Bunker | Hide on person                 | Second NMT in TPR  | M  | H  |
|      |               |                           | Hide with tools or equipment   | Second NMT in TPR  | M  | H  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      | M  | M  |
| 5    | PA            | Remove target from PA     | Hide on person                 | SNM and Metal Portals, Hand search                         | H  | H  |
|      |               |                           | Hide with tools or equipment   | SNM portal, X-ray, Hand search                             |    |    |
|      |               |                           | Hide in vehicle with shielding | Contamination and SNM check, Hand search                   |    |    |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      |    |    |
|      |               |                           | Throw over fence               | CCTV, General observation, Random patrols, 20 m clear zone |    |    |

# Methodology for Evaluating the Protection System

---

1. Develop a sequence of adversary actions for each target



2. Identify measures that protect against these actions



3. Characterize protection measures



4. Develop vulnerable paths



5. Develop worst case scenarios

# Identify Vulnerable Protection Measures

---

- **Review the likelihood of detection and assessment for each step**
- **Identify vulnerable protection measures**
  - **Select lowest probability of detection and assessment for each area**
- **Develop vulnerable paths for threat/target combinations**
  - **Combine various insider actions and protection elements to create insider theft scenarios**

# The Adversary Optimizes the path to Acquire and Remove Material

---

- **Select the best strategies to traverse each protection layer**
  - The insider must defeat one of more protection measures at each step
- **Select the best combination of each path element to construct a complete path out of the facility**
  - The insider actions must traverse each layer of protection
- **Several insider path combinations may be equally vulnerable**
  - Each combination must be evaluated independently
- **Timing and quantities of target material selected in attempt to defeat MC&A systems**

# Adversary Chooses Strategy That Minimizes Probabilities of Detection and Assessment

| Step | Area          | Actions                   | Insider Strategies             | Existing Protection Measures                               | Pd | Pa |
|------|---------------|---------------------------|--------------------------------|--|----|----|
| 3    | Inside Bunker | Acquire Target            | Hide on person                 | Second NMT in TPR  | L  | M  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      | L  | L  |
| 4    | Bunker        | Remove target from Bunker | Hide on person                 | Second NMT in TPR  | M  | H  |
|      |               |                           | Hide with tools or equipment   | Second NMT in TPR  | L  | H  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      | M  | L  |
| 5    | PA            | Remove target from PA     | Hide on person                 | SNM and Metal Portals, Hand search                         | H  | H  |
|      |               |                           | Hide with tools or equipment   | SNM portal, X-ray, Hand search                             | L  | M  |
|      |               |                           | Hide in vehicle with shielding | Contamination and SNM check, Hand search                   | L  | M  |
|      |               |                           | Falsify shipment               | MC&A shipment procedure, MC&A records                      | M  | M  |
|      |               |                           | Throw over fence               | CCTV, General observation, Random patrols, 20 m clear zone | L  | M  |

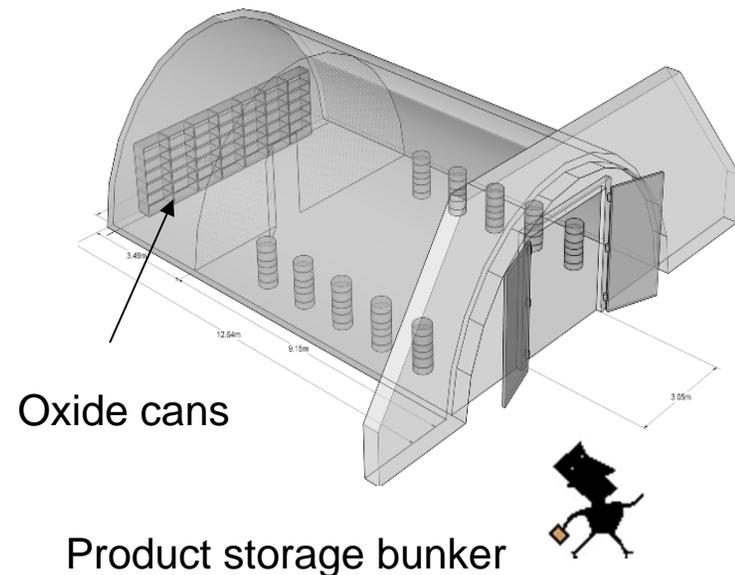
# Two Methods to Combine Qualitative (H,M,L) Scores

---

- **Expert Opinion – consider the detection and assessment event and assign an overall score**
  - **Pro: Can account for many subjective and complex factors**
  - **Con: Evaluations may not be consistent from one target to another and it does not scale to hundreds of scenarios**
- **Numerical encoding**
  - **Map H, M, L into probability scale and perform math**
  - **Pro: Consistent and transparent scales**
  - **Con: Does not capture additional information or expert judgment**
- **May be best to use a combination of the two approaches**

# Estimate Measure Effectiveness Summary

- To estimate the effectiveness of each insider protection measure:
  - Define possible methods of detection and assessment based on insider theft actions/strategies
  - Estimate the detection and assessment likelihood of each measure based on insider theft actions/strategies



# Methodology for Evaluating the Protection System

---

1. Develop a sequence of adversary actions for each target



2. Identify measures that protect against these actions



3. Characterize protection measures



4. Develop most vulnerable paths



5. Develop worst case scenarios

# Determining Worse Case Scenarios

---

- **Determining worse case scenarios is an iterative process that must consider various:**
  - **Target material types/forms/locations**
  - **Insider types and capabilities**
  - **Physical and administrative protection measures verses insider strategies**
  - **Facility conditions and processes**

# The Adversary Optimized path to Acquire and Remove Material

| Step | Area          | Actions                   | Insider Strategies           | Existing Protection Measures          | Pd | Pa |
|------|---------------|---------------------------|------------------------------|---------------------------------------|----|----|
| 3    | Inside Bunker | Acquire Target            | Falsify shipment             | MC&A shipment procedure, MC&A records | L  | L  |
| 4    | Bunker        | Remove target from Bunker | Falsify shipment             | MC&A shipment procedure, MC&A records | M  | L  |
| 5    | PA            | Remove target from PA     | Hide with tools or equipment | SNM portal, X-ray, Hand search        | L  | M  |

# Module Summary

---

- **Estimated the effectiveness of each protective measure**
- **Characterized the protective measures at the URF**
- **Established likelihood of detection and assessment for each step**
- **Identified most vulnerable protection measures**
- **Developed most vulnerable paths for threat/target combination**

# Exercise 12: Characterize protection measures and evaluate scenarios

---

- **Complete the worksheets:**
  1. **Define alternative insider actions and strategies that could be used at each step in the scenario**
  2. **Describe existing protection measures that could detect adversary for each step in the scenario**
  3. **Estimate probability of detection ( $P_d$ ) and probability of correct assessment ( $P_a$ ) for each step (H, M, or L)**
  4. **Identify the best insider strategy for each step in the scenario**
  5. **Describe the optimal scenario**
- **Present summary to the large group**





# Lecture 13

---

## Protracted Theft Analysis



# Learning Objective

---

- **Recognize situations/opportunities for protracted theft strategies**
- **Review methodology for analysis of protracted theft**
- **Apply methodology to URF**

# Material accounting (MA) systems provide delayed detection capability against protracted theft

- MA systems may not be effective for *prompt* detection of abrupt theft
- Bulk material inventory differences exceeding acceptable limits or a discrete item not in its authorized location when needed for processing may provide *delayed* detection
- Need to take into account
  - Measurement errors
  - Timing of protracted theft activities and subsequent MA activities
  - Potential insider subversion of or tampering with MA safeguards
  - Potential differences in effectiveness of subsequent MA activities if the first occurrence failed to detect theft



# Alternative protracted theft strategies and protection elements must be examined

|   | Step                      | Strategies                                   | Protection elements         |
|---|---------------------------|--|-----------------------------|
| 1 | Acquire target protracted | 5 acquisitions<br>1,000 g each<br>1 day each | Access and material control |
|   |                           |  | Day measurements            |
|   |                           |  | Weekly trending             |
|   |                           | 10 acquisitions<br>500 g each<br>1 day each  | Access and material control |
|   |                           |  | Day measurements            |
|   |                           |  | Weekly trending             |
|   |                           | 20 acquisitions<br>250 g each<br>1 day each  | Access and material control |
|   |                           |  | Day measurements            |
|   |                           |  | Weekly trending             |
| 2 | Remove from MAA           | ECP  | Personnel entry/exit        |
|   |                           | Clean waste                                  | Confirmatory check          |
|   |                           | Rad waste                                    | NDA measurement             |
| 3 | Remove from PA            | ECP  | Personnel entry/exit        |

# There are three primary detection opportunities for protracted theft scenarios

---

## 1. Detect during each acquisition of material

- Access control (e.g., badge reader)
- Material control (e.g., two person rule)

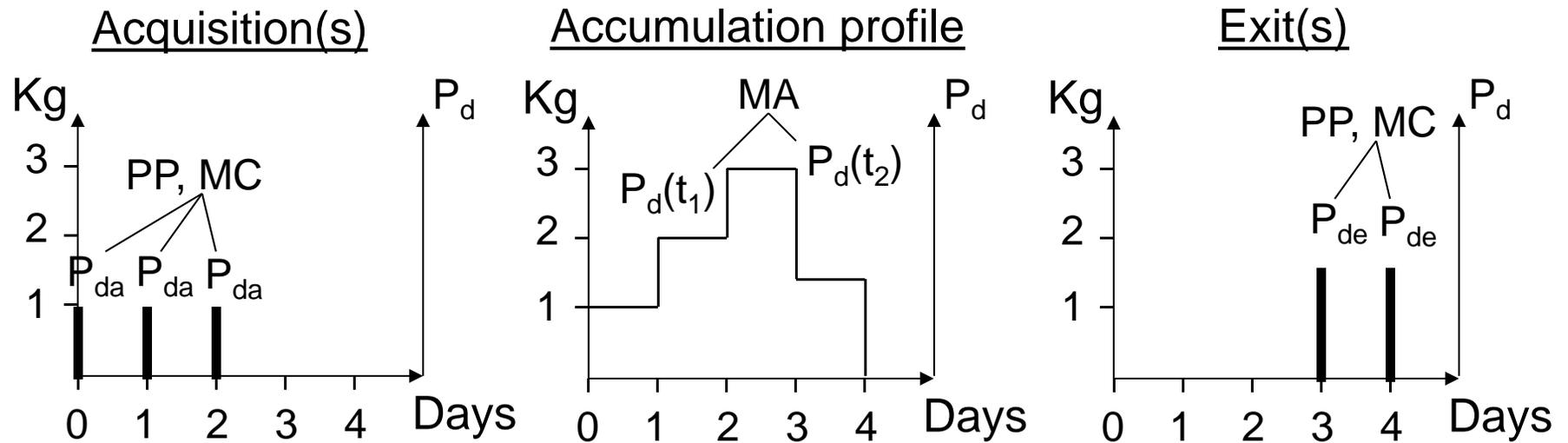
## 2. Detect reduction in inventory during scenario

- Periodic physical inventory taking, process calls or material transfer checks may reveal absence of material
  - Material transfers could be within MBA, between MBAs or off site

## 3. Detect during illicit removal from site

- Material control (e.g., material transfer forms)
- Access control (e.g., fence and other physical barriers)
- Physical protection (e.g., radiation portal monitors)

# The three phases of protracted theft can be detected with PP, MC and MA systems



Each abrupt removal to staging area could be detected with access and material control systems ( $P_{da}$ ).

Periodic or random inventories at  $t_1$  and  $t_2$  could detect missing material or material out of place.

Each abrupt removal from site could be detected with physical protection and material control systems ( $P_{de}$ ).

PP – physical protection, MC – material control, MA – material accounting

# Specify the parameters of the protracted theft scenario

1. Insider access, knowledge and authority – determines  $P_d$  during acquisition
2. Timing of acquisitions – time required for each acquisition, time interval between acquisitions, number required for goal quantity
3. Accumulation area
4. Timing of exit activities – time for each exit, number of exits, time interval between exits

The screenshot shows a dialog box with the following fields and controls:

- Title:** Define multiple acquisitions / exits
- Personnel:** A list box containing 'SI', 'Operator', and 'Health Physicist'. 'SI' is selected.
- Time for each acquisition activity:** Input field with value 0.
- No. of acquisitions to accumulate target:** Input field with value 4.
- Interval between acquisitions (days):** Input field with value 3.
- Accumulation area:** A list box containing 'Limited Area'.
- Time for each exit activity (days):** Input field with value 0.
- No. of exits with portions of material:** Input field with value 1.
- Interval between exits (days):** Input field with value 0.
- Buttons:** 'Get help', 'OK', and 'Cancel'.

# Specify material accounting activities

- Inventory and production schedules
  - Inventory sampled or required for production (%)
  - Time between inventories or process calls – scheduled or average time between random inventories
- Effectiveness
  - $P_d$  for each adversary type - may be small or zero if the insider is responsible for conducting inventories or maintaining records
  - $P_d$  for first inventory
  - $P_d$  for each subsequent inventory – overall probability of detection will increase over time as more material is diverted

**Define Material Accounting Activities**

Name:

Time interval in:

Activity Is:  
 Scheduled  
 Random

Target location:

| Personnel        | Pd 1st | Pd 2nd |                                  |
|------------------|--------|--------|----------------------------------|
| SI               | 0.20   | 0.20   | <input type="button" value="↓"/> |
| Operator         | 0.20   | 0.20   | <input type="button" value="↓"/> |
| Health Physics   | 0.20   | 0.20   | <input type="button" value="↓"/> |
| Maintenance      | 0.20   | 0.20   | <input type="button" value="↓"/> |
| Production Super | 0.20   | 0.20   | <input type="button" value="↓"/> |

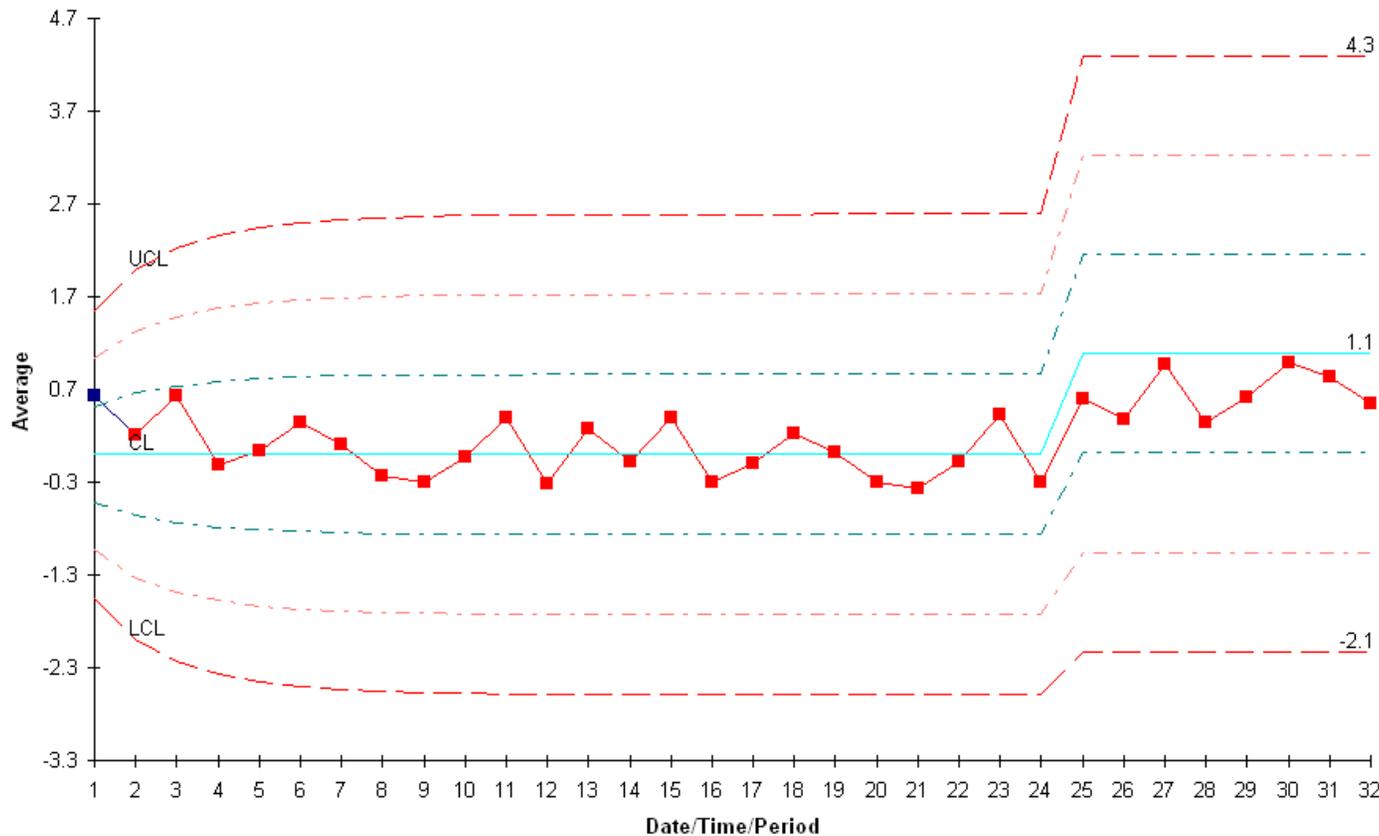
Pd per: 1  2

# Trend Analysis is Used to Detect Protracted Theft Attempts

- Use cumulative sum (CUSUM) statistical tests
  - Sum likelihoods of observed inventory differences assuming normal material unaccounted for (ID) distribution
    - ID distribution may have negative mean caused by process hold up
    - Variance of ID distribution may change due to equipment modifications or environmental variables
  - Initiate alarm when sum exceeds threshold
    - Or change in slope
    - Or sequence of points near alarm limit
    - Or change in process variance
- For a sequence of two IDs
  - $ID_1 = PB_1 - PE_1 + X_1 - Y_1$
  - $ID_2 = PB_2 - PE_2 + X_2 - Y_2$
  - Do not expect successive IDs to be independent ( $PE_1 = PB_2$ )

# EWMA or CUSUM statistical tests typically used for trend analysis

- Inventory difference drifts down during protracted theft
- Measurements have error distributions shown
- Probability of detection may change over time

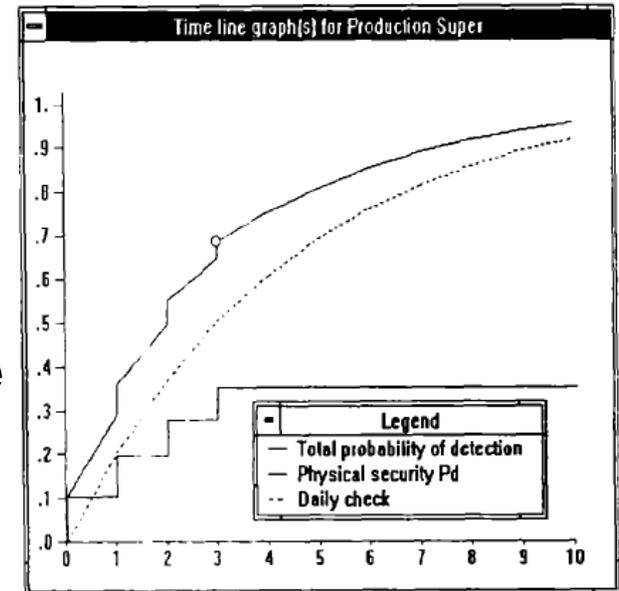


No

ecture 13-10

# Protracted theft scenario analysis incorporates PP, MC and MA factors

- Acquisition and exit events
  - Use abrupt theft techniques
- Material accounting system
  - Compute cumulative probability of detection during protracted theft timeline
- Overall probability of detection for scenario is:



$$P_d = 1 - (1 - P_{da})^n \times (1 - P_d(t))^i \times (1 - P_{de})^m$$

Avoid detection during n acquisitions

Avoid detection during i balance periods

Avoid detection during m exits

- Perform for each adversary, location and scenario

# Summary of protracted theft analysis steps

---

- 1. Define alternative protracted theft scenarios (number of acquisitions, staging area, exit attempts and timing of each)**
- 2. Identify layers and physical protection elements that would detect acquisitions and exits**
- 3. Identify material accounting elements that would detect missing or staged materials**
- 4. Identify alternative strategies for each adversary action**
- 5. Evaluate effectiveness of each element against each adversary action**
- 6. Choose best strategy at each layer**

# Exercise: Estimate Pd for alternative protracted theft scenarios

|   | Step                      | Strategies                                   | Protection elements  | Pda | Pd(t) | Pe |
|---|---------------------------|--|----------------------|-----|-------|----|
| 1 | Acquire target protracted | 5 acquisitions<br>1,000 g each<br>1 day each | Access/matl. control |     |       |    |
|   |                           |  | Day measurements     |     |       |    |
|   |                           |  | Weekly trending      |     |       |    |
|   |                           | 10 acquisitions<br>500 g each<br>1 day each  | Access/matl. control |     |       |    |
|   |                           |  | Day measurements     |     |       |    |
|   |                           |  | Weekly trending      |     |       |    |
|   |                           | 20 acquisitions<br>250 g each<br>1 day each  | Access/matl. control |     |       |    |
|   |                           |  | Day measurements     |     |       |    |
|   |                           |  | Weekly trending      |     |       |    |
| 2 | Remove from MAA           | ECP  | Personnel entry/exit |     |       |    |
|   |                           | Clean waste                                  | Confirmatory check   |     |       |    |
|   |                           | Rad waste                                    | NDA measurement      |     |       |    |
| 3 | Remove from PA            | ECP  | Personnel entry/exit |     |       |    |



# Lecture 14

---

## Upgrade Analysis



# Learning Objective

---

- **In this module we will:**
  - **Discuss the importance of, and a process for, upgrade selection**
  - **Discuss examples of effective system enhancements**

# **There is a four step process for identifying effective upgrades**

---

- 1. Identify system strengths and weaknesses for the spectrum of threats**
- 2. Identify safeguards upgrades that address individual weaknesses**
- 3. Package the alternative upgrades for meaningful analysis of their benefits**
- 4. Estimate costs and operational impacts of these upgrades packages; rank them**

**These should be considered for all threat/target combinations.**

# 1. Identify system strengths and weaknesses for the spectrum of threats

---

- Consider all insider types, targets and theft strategies
- Examine optimal (highest risk) strategies or scenarios and ones that are similar
  - Identify insider actions that are not effectively detected by existing protection measures in many of the scenarios
  - Perform defense-in-depth analysis to help identify critical components
  - A critical component is one whose failure would dramatically decrease performance
- Remember that when one security flaw is fixed insider can switch to a different strategy

**It is important not to focus only on "worst case" results.**

# Examining the evaluation results to identify weaknesses in protection measures

---

| Location/measure                    | Weaknesses   |
|-------------------------------------|--|
| Target location<br>Chip vault-shelf | Many insiders with access to material  |
| Process Area<br>Emergency exit      | Insider can actuate fire or criticality alarm<br>Evacuation requires rapid departure<br>Actuate alarm, remove material, throw over fence |
| Protected Area<br>Vehicle portal    | Shield in vehicle<br>Piggyback<br>Disguise as sample or waste  |
| Process area<br>MC&A system         | Difficult to determine which operation is causing an inventory difference (ID) and large uncertainty on difference                       |

## 2. Identify safeguards upgrades that address individual weaknesses

| Location/measure                     | Weaknesses   | Potential upgrades   |
|--------------------------------------|--|--|
| Target location<br>Chip vault -shelf | Insider access                                       | Enhanced 2 person rule - Add cages                           |
| MAA<br>Emergency exit                | Evacuation control                                   | CCTV<br>Emergency Inventory<br>Better criticality alarm      |
| PA<br>Vehicle portal                 | Shield in vehicle<br>Piggyback<br>Disguise as sample | Vehicle search<br>Cart and carrier search<br>Verify transfer |
| Process area<br>MC&A system          | Cause of ID and large uncertainty                    | Restructure MBAs to better localize IDs                      |

# Upgrades will vary in their benefits and ease of implementation

---

- Some vulnerabilities are easy to fix in a timely manner
- Combinations of hardware and procedural upgrades are often needed
- Procedural upgrades are often less costly and easier to implement than changes in facility or hardware
- An upgrade to address a given vulnerability may introduce a new one
- An upgrade may cause insider to switch to another strategy that is almost as effective

Careful analysis should be performed prior to implementing any proposed upgrades

### **3. Package the alternative upgrades for meaningful analysis of their benefits**

---

**Organize by theft stage:**

**SNM Acquisition**

**MAA Removal**

**PA Removal**

**MC&A system (protracted)**

**Organize by ease of implementation:**

**Quick Fix (cheap)**

**Moderately Expensive**

**Most Expensive**

**Upgrades can be organized by theft stage addressed and ease of implementation.**

# Process for identifying upgrade packages

---

- **Identify candidate upgrade packages**
- **Repeat vulnerability assessment with upgrades in place, get new estimates of system effectiveness and risk (increase in Pd)**
- **If upgrades achieve acceptable risk, conduct cost-benefit analysis**
- **If upgrades do not achieve acceptable risk, identify additional upgrades and repeat**

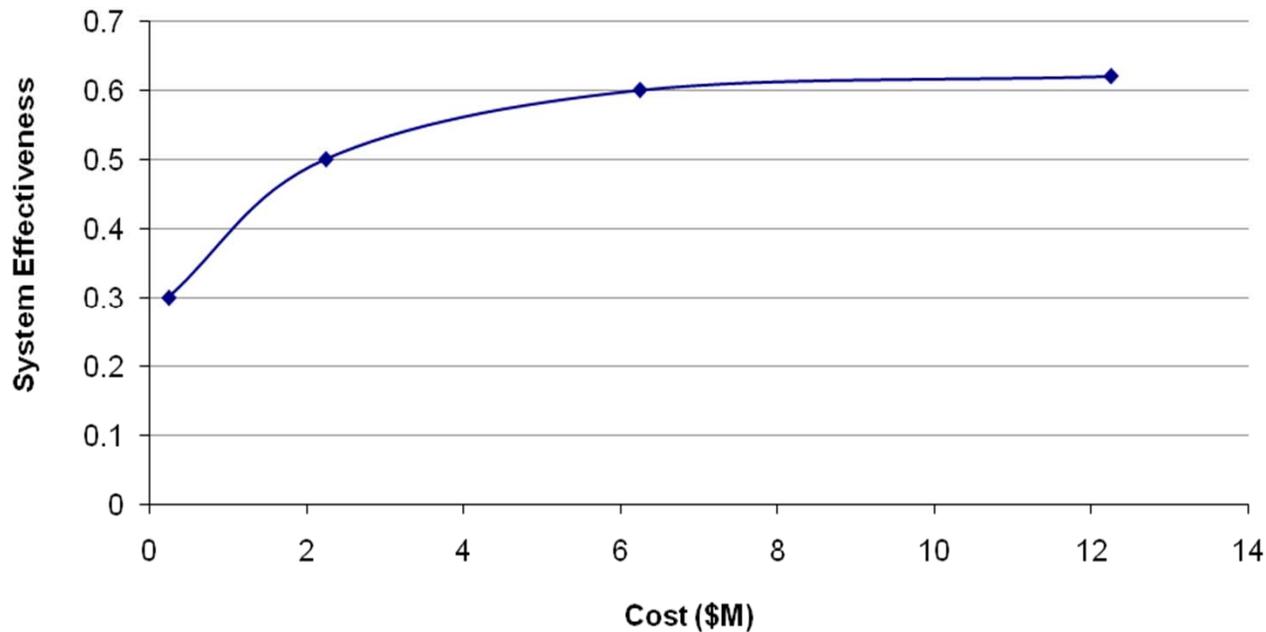
## 4. Estimate costs of upgrades packages; rank them by effectiveness-cost ratio

|                    |   |
|--------------------|---|
| Onetime costs      | Design<br>Equipment<br>Installation                                     |
| Recurring costs    | Operation<br>Maintenance<br>Repair<br>Replacement                       |
| Non-monetary costs | Production impact<br>Health and safety<br>Employee morale<br>Aesthetics |

$$\text{Effectiveness-cost ratio} = (\text{Increase in Pd})/\text{Cost}$$

# Cost benefit ratios can be computed for alternative upgrade packages

| Safeguards package | Cost (\$M) | Effectiveness (increased Pd) | Effectiveness/cost | Cumulative cost | Cumulative benefit |
|--------------------|------------|------------------------------|--------------------|-----------------|--------------------|
| Vault upgrades     | 0.25       | 0.3                          | 1.2                | 0.25            | 0.3                |
| Emergency exit     | 2          | 0.2                          | 0.1                | 2.25            | 0.5                |
| Vehicle portals    | 4          | 0.1                          | 0.025              | 6.25            | 0.6                |
| Fenceline          | 6          | 0.02                         | 0.003333333        | 12.25           | 0.62               |



# More complex procedures can be used to optimize upgrades

---

- **Budget or logistical constraints may prevent immediate implementation of desired upgrades**
- **Tradeoff between addressing different types of threats can be calibrated using multiattribute utility function**
- **Optimization algorithms to allocate available resources to upgrade implementation over time**
- **Example: Prioritizing and Scheduling Safeguards and Security Upgrade Projects Under Restricted Budgets, UCRL-JC-110105, Edmunds, et. al., INMM 33<sup>rd</sup> Annual Meeting, 1992**

# Summary

---

- Discussed ways to bundle groups of upgrades
- Evaluated effectiveness of each group of upgrades
- Select groups with highest effectiveness-benefit ratio



# Lecture 15

---

## Maintaining System Effectiveness



# Learning Objective

---

- **In this module we will discuss:**
  - **How insider threat mitigation strategies are assured through:**
    - **Self-assessments,**
    - **Performance testing of key systems,**
    - **Oversight activities**
- **Short video exercise**

# Self-Assessment Programs

---

- **To maintain system effectiveness, each site should conduct self-assessments administered through a formal program.**
  - **Best accomplished through an independent objective organization**
  - **Assessment program plan and performance of the plan are subject to annual review**
  - **Programs should assess MPC&A functions deemed critical by a vulnerability assessment**
- **Without evaluating your system's effectiveness, you cannot have a high confidence that your facility is protected against insider (and outsider) threats.**

# Performance Testing

---

- **Performance testing is an integral part of self-assessments. Testing should focus on:**
  - **Individual MPC&A elements considered critical to detection and/or mitigation of theft or diversion scenarios, and**
  - **Multiple MPC&A elements (systems) based upon defined theft or diversion scenarios**
- **Personnel and systems are periodically tested according to an approved plan**

**Response Force functions are also included as part of PP testing**

# Benefits of a Testing Program

---

- **Determines the effectiveness of the safeguards and security program elements**
- **Determines effectiveness of individual critical protection elements**
- **Identifies system strengths and weaknesses**
- **Validates vulnerability analysis**
- **Validates procedures**
- **Validates training effectiveness**

# Benefits of a Testing Program

---

- **Promotes continuous improvement of protection systems**
- **Produces data for lifecycle management**
- **Provides data for financial analysis for continued support/upgrades**
- **Promotes quality by supporting improvement initiatives**
- **Integrates MC&A and physical protection**

# Key MPC&A Elements for Testing

- Access control systems and procedures
- Surveillance systems and procedures
- Administrative procedures
- Detection sensors
- Process control systems and procedures

- Inventory systems and procedures
- Measurement systems and procedures
- Accounting systems and procedures
- Material Transfer procedures
- Health and safety systems and procedures

**The Emergency Management System should also tested**

# Element Evaluation Approaches

---

- **Standard requirements**
- **Performance tests**
  - **Functional tests**
  - **Effectiveness tests**



It is essential to analyze performance test data in order to: 1) support insider analyses; 2) validate effectiveness of protection programs; 3) validate the VA and its assumptions; 4) validate training & procedures

# Standard Requirements

---

**For many system elements, standard requirements may already exist, or can be created.**

**They should assure that:**

- **The inherent capabilities of the protective system will be fully realized.**
- **Protective systems are working at their intended/required level of performance.**
- **The protective system functions consistently and reliably.**
- **Malfunctions and failures are detected and corrected in a timely manner.**



# Expert Judgment

---

- **The effectiveness of many detection elements, especially those relying on human factors, may be difficult to quantify by testing.**
- **Additionally, determining what elements to test and how often requires a lot of coordination between departments.**
- **Here the collective judgment of knowledgeable and experienced individuals will be of value.**
- **Sites often form Performance Test “Boards” to determine what to test and to set test parameters (desired effectiveness levels)**
  - **The approach should be carefully structured**
  - **It should draw on individuals from all relevant areas**

# Performance Tests

---

The security manager typically wants to know two things about the protective system: Are the systems functioning and are they functioning at the required level of effectiveness.

- **Functional tests**: Determine that the element is operating
  - “does it work or not”
- **Effectiveness tests**: Determine that element and/or system of elements are operating at intended level of effectiveness
  - “how well does it work”

**The selection, design, and execution of performance tests and the analysis of their results requires a carefully structured approach.**

# Limited Scope Testing

- **Prior to a full-scale exercise, certain system elements can be examined or evaluated with limited-scope performance tests**
  - **Alarm systems**
  - **Emergency situations**
  - **Material control measures**
  - **Waste streams**
  - **Effectiveness of area searches**
  - **Transfer procedures**



# System/Subsystem Testing

- Higher and more complex level of performance test
- Evaluates:
  - Individual protection elements
  - Elements within a critical path
  - The interaction/integration of the individual elements
- Includes equipment and personnel
- Usually based on one of the scenarios identified in a vulnerability assessment – such as an insider threat scenario



# Performance Tests – Selection

---

**Since resources are limited, tests should be selected which will provide the most useful information about critical protection elements. Important considerations include:**

- **Testing program should be organized to produce the greatest number of data points with the least impact on resources and operations**
- **Components and systems that have the greatest impact on reducing risk should be tested more frequently**



# Performance Tests – Design

---

The design of performance tests involves a number of important considerations:

- **Scope**
- **Test conditions**
- **Test environment**
- **Test scenario**
- **Control of variables**
- **Test controls**
  - **Facility area and personnel participation**
  - **Notification plans**
- **Reporting Test results**



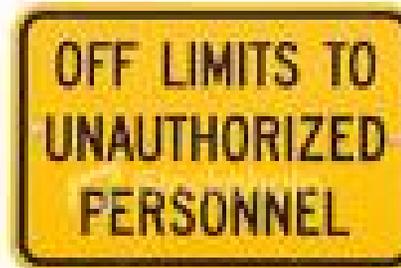
**Plan carefully**

# Performance Tests – Constraints

---

**A number of considerations may affect how tests are performed:**

- **Unacceptable impact on operations**
- **Personnel Health or safety issues**
- **Labor/management agreements and relations**
- **Unacceptable risk to materials or assets**



# Performance tests – Evaluation

---

**After the completion of a test, an evaluation must be carried out to reach certain conclusions:**

- **Achievement of test objectives**
- **Applicability of results**
- **Indications of deficiencies or vulnerabilities**



# Summary

---

- **A well designed Performance Testing Program serves as the vehicle to determine the health of the safeguards and security system.**
- **For each critical protection element, equipment, procedures, personnel and system integration must be considered.**
- **The performance testing program is a continuous process.**
- **Without performance testing, the effectiveness of insider threat mitigation strategies is not really known.**

# Video Exercise

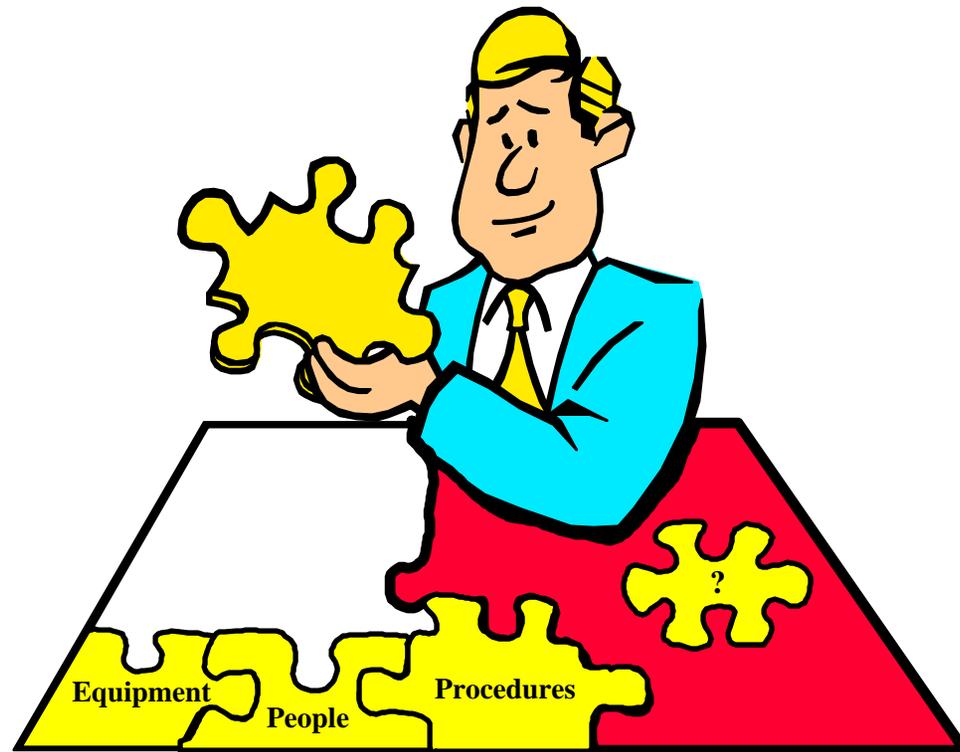
---

- **Watch the video and we will discuss the results**

# Summary

---

- Questions and Answers





# Lecture 16

---

## Group Discussion



# Learning Objective

---

- **Identify Trends in Insider Protection**
- **Identify Concepts for Collaboration**



# Lecture 16

---

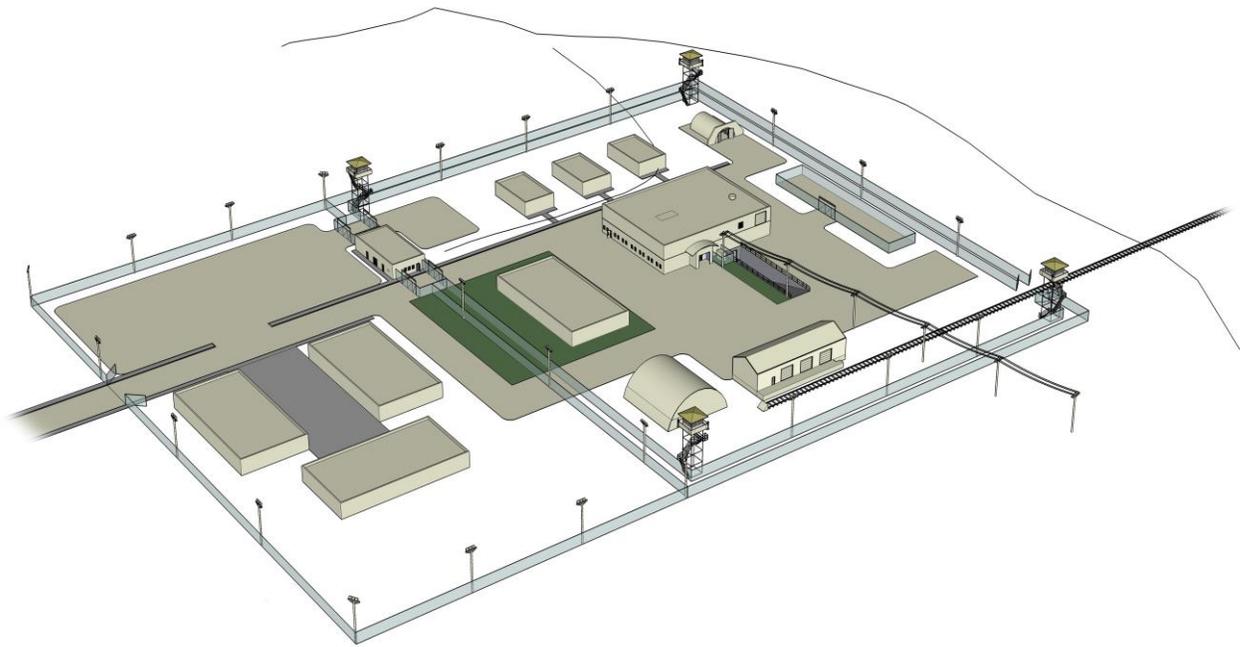
## Course Conclusion



# Learning Objective

---

- **Presentation of Certificates**
- **Closing Remarks**



**Exercise 2**  
**Hypothetical Facility Overview**  
**Role play Text**

**Plant Manager Overview:** Good afternoon. I am the Plant Manager. I'll give you an overview of the plant operations. You can find more details in your handbook about the site. At the end I'll be happy to answer your questions. First let me tell you some things about our site:

The Uranium Research Facility (URF) is a national defense facility for the manufacture of uranium billets used in research. During normal operation, 250 full-time employees work at the site in plant operations, maintenance, engineering, technical support, management and administrative support positions. Of these, 182 employees require some access to the Protected Area (PA).

The site, which is located in a semi-arid high desert, is divided into two main areas. The first is the low security Administration Area, where much of the non-production activities take place. Approximately 30% of the staff works in this area. The second area is the PA. This very high-security area contains the main fabrication buildings, the production support buildings, storage vaults, road and rail transportation terminus, and the main cafeteria.

The main product of the URF is high-quality uranium billets that are used in nuclear material research. The input stream of this process begins with the delivery of uranium dioxide (UO<sub>2</sub>) powder. This powder is processed into raw ingots through a casting process. The raw ingots are then further processed into standard billets of specific size, shape, and weight. The waste from these processes goes into a uranium recovery stream that reintroduces the scrap material into the input stream. The finished product undergoes quality assurance (QA) checks and is then stored at a bunker until it is transported by rail or truck to end users.

The northern two-fifths of the URF Site is the Administrative Area (AA). This area is surrounded by a fence along three sides—known as the North Fence—and the PA fence along the southern side.

The buildings in the AA are unlocked except on weekends and holidays. Most senior management personnel have keys to the outer doors of these buildings. Personnel all have keys to their specific work areas. All keys are controlled by the guard force and are stamped "Do not duplicate."

The buildings of the AA are not alarmed, except for the analytical lab on the first floor of the building nearest the PA. The guard force responds to any alarms that occur in this area. Members of the guard force have a master key that allows them to enter and investigate the analytical lab after an alarm occurs.

There are nine buildings inside the PA perimeter. The main production building is the Process Facility located near the center of the area. There is also an Entry Control Building (ECB) that straddles the northern perimeter and houses pedestrian and vehicular entry control points, the CAS, and the Response Force Ready Room. Material shipments are processed through the shipping and receiving building. This building can support both road and rail transports. A storage bunker, located in the southeast corner of the PA, is used to store finished products prior to shipping. A full service x-ray diagnostic facility, located in northwest corner of the PA, is used for product quality control inspections. The PA also houses several small office buildings and the main cafeteria.

All manufacturing processes are contained within the URF Processing Building. This building is a multi-story facility with a basement, ground, and mezzanine level. It has a total area of approximately 1700 square meters. The partial basement is the machine cooling fluid processing area, the ground floor is the processing area, and the mezzanine is the heating, ventilation, and air conditioning (HVAC) area. The production areas of the building are under negative pressure and all ventilation from these areas is passed through high efficiency particulate air (HEPA) and/or charcoal filters to minimize plant releases.

The URF Processing Building houses the following areas/operations:

- Casting Furnace Area—This area holds the two furnaces where UO<sub>2</sub> power is cast into ingots.
- Billet Vault—Finished ingots are stored here until needed by machining process.
- Special Nuclear Material (SNM) Machining Area—This area holds nine milling machines that can be configured to work as three lines of a three-step milling process or as nine individual stations. The milling process converts raw ingots to finished billets.
- Product Vault—This vault stores finished billets before they are sent to QA or to the Storage Bunker.
- QA Vault—In-process billet samples and final products are measured and tested in this vault. Only a limited amount of material may be in this vault at any one time.
- AA—The Administrative Area is the general office area.
- Chip Vault—This vault stores return stream waste from the Casting Furnace and Machining areas before it is reintroduced into the input stream.

The Shipping and Receiving building (23 in Figure 1-2) is a one-story building with loading docks on both sides (one for rail shipments and one for trucks). Although several cubical office spaces are inside, it is basically an open warehouse.

The Bunker (20 in Figure 1-2) is used to store nuclear material that was shipped in for recycling, and finished products that are packed and ready to ship.

There are three single-story Support Buildings that house offices and light laboratory facilities. These Support Buildings, located east of the Processing Building (17, 18, 19), store some classified material in safes. Nuclear material is not brought into these buildings.

Now, I'll be happy to answer your questions.

**MC&A Manager Overview:** Good afternoon. I am the Site MC&A Manager. I'll give you an overview of the site MC&A program. You can find more details in your handbook about the site. At the end I'll be happy to answer your questions. First let me tell you some things about our program.

By letter of designation, the plant manager has delegated the responsibilities and authorities of all safeguard positions. A single individual is assigned the responsibility for technical coordination of the overall MC&A program. This position is referred to as the Material Control Manager. This is me. This position is separate from production and any other responsibilities that might give rise to a conflict of interest. In addition, there is a Measurement Control Coordinator, and, if needed, multiple Material Balance Area (MBA) Custodians assigned specific authorities, responsibilities, and locations reporting directly to the Material Control Manager.

Three MBAs have been established at the URF. These are the Production Floor, the X-Ray Facility, and the Final Products Bunker. All SNM at the URF is maintained in one of these three MBAs. The physical boundaries of the X-Ray Facility and the Final Products Bunker MBAs are the structural boundaries of the respective building. The physical boundaries of the Production Floor MBA are the walls and access control point for the production area.

The Measurements and Measurement Control program is under the control of the Measurement Control Coordinator. The measurement control program is expected to establish and verify inventory quantities and to ensure the quality and reliability of the measurement data. This facility would incorporate the following measurement control elements:

- various mass weighing stations
- destructive laboratory analysis and sampling
- non-destructive analysis (NDA) measurement systems
- weekly calibration or operability checks with reference standards
- a sampling program to ensure that portions of the bulk material taken for measurement are representative of the bulk material
- control programs associated with all measurement systems to assure the quality of data generated

The measurement Control Coordinator maintains the equipment and standards in a locked room in the non-nuclear material portion of the processing facility and is responsible for the proper use and calibration of the equipment.

In addition, the MC&A organization would control and issue TIDs for use throughout the facility. MBA Custodians would be the only personnel trained to apply and remove TIDs.

A physical inventory is conducted every two months under normal conditions. This physical inventory consists of a 100% inventory of items or containers with TIDs, and measurement of a statistical sample of items. The measurements are NDA measurements and the attributes are compared to the book data. Discrepancies are tracked in the measurement control system. If a measurement is beyond the control limits for that

measurement from the recorded value, the item in question is subjected to additional confirmatory measurements, including opening the container and, if required, conducting destructive measurements.

Data obtained during the physical inventory, data from measurements during the material reconciliation period, and control program data are used to calculate the Limit of Error of Inventory Difference (LEID). Special inventories are conducted when custodial responsibilities are changed, items are believed to be missing, inventory differences exceed established control limits, and other abnormal occurrences take place. These special inventories may be limited to a single vault or MBA, depending on the occurrence. However, the facility may be impacted, depending on the circumstances. Investigation of inventory differences between accounting records and physical inventory results will be performed to determine the cause.

Material measurements may take place at several points in an item's life in the processing area. Material is normally measured on the following occasions:

- A receipt measurement is taken within five days of receipt.
- Depending on whether the mass limit exceeds 2 kgs, an item may require a measurement for Internal Transfers between MBAs.
- Measurements are taken when modifications are made to materials in the machining or casting process.
- Measurements are taken as part of Item Monitoring along the process path.
- Final product measurements are taken before containerization and TID application.
- A final measurement is performed within five days before shipment.

Items received are booked on shipper's values for element and isotope content. When shipments are received, the item count and item identifiers are verified against the shipping documents. Items shipped are sent based upon the book values for the element and isotope content. Where shipper receiver differences are identified on shipped items, the shipper-receiver difference is resolved by adjusting the URF book values to the receiver's measured values, as long as the difference does not reflect a difference in the number and identity of the items shipped and received.

In addition to the fixed periodic physical inventories, the process area has further designated several Inventory Control Locations, which provide the capability to physically locate (or confirm the location of) items in a timely manner. This capability to localize losses (or thefts) of SNM allows for the identification of the mechanism/s for any such loss (or theft) in a more time-sensitive manner. Process boundaries are selected primarily on the basis of manufacturing control; however, this division also enables managerial assignment of specific material handling and control responsibilities, if required.

URF submits material balance reports for each MBA within 30 days of completion of a physical inventory. Nuclear material transaction reports for the MBA covering all transactions during the inventory period are submitted with the material balance report. URF provides a telephone report to the State regulator within four hours of determining that an item cannot be accounted for. This report is followed up by a written report within 24 hours of this determination.

URF employs a computer-based accounting system that is managed and operated by personnel who are not authorized access to SNM. The computer on which the accounting system is run is a standalone machine. Entry of or access to accounting data or modification of the accounting software requires authorization via a password system. All data is input to the URF computer accounting system from paper records (e.g., inventory sheets and material transfer forms), which are uniquely numbered, accounted for, signed by the individuals completing them, and retained for the life of the plant. The URF accounting software is commercially procured and is not modified by plant staff.

Physical control of the material is established through several individual programs. Access controls limit personnel access to the processing area, and additional access controls further limit personnel access to the processing floor in the processing building. Once on the processing floor, procedural measures limit access to material to those with an established need for access. The MBA Custodians for the various process area locations authorize all material movements. Material access is further enforced through the use of the two-person rule. Any time a material location is accessed, two persons must be present. Two persons must also be present when material is on the machines on the process floor. The machine operator is one of the two persons and the machining supervisor or MC&A representative acts as the second person for all material being worked on at any given time. Access to specific parts is controlled through the use of locks on the birdcages containing materials. The machine operator is only issued the keys for the work that is at his station for the day

Personnel entering the PA must process through the ECP. The ECP is open from 0700 to 1800 Monday through Friday. Authorized personnel enter the area through the middle double doors to the ECP and process through contraband portal detectors. All hand-carried items are placed in plastic boxes and processed through the X-ray machine. Personnel then proceed through the portal metal detector. If they trigger an alarm, they may walk back through the portal, search themselves to determine what caused the alarm, place that material on the X-ray belt, and walk through the portal again. If they do not trigger another alarm, they may collect their materials and enter into the processing area. If they set off the portal alarm a second time, they must be searched by the guards with a hand-held unit. The guards also monitor the X-ray video for contraband. There are two guards at the portal area to process personnel.

Personnel exiting the PA enter the ECP through the double doors and pass through the nuclear material monitoring portal. If they do not set off the alarm, they continue through the exit doors (east and west). If there is an alarm, the guards will stop the person passing through the alarming portal and call the Health Physics personnel, who will respond to determine the cause of the alarm. If the portals alarm when personnel are passing through them to enter the area, the person is stopped and questioned regarding possible reasons the alarm might have gone off and Health Physics is called to check the equipment. That exit door will be locked until the monitor is certified to be in working order.

The ECP for the processing floor in the processing building is similar to the area ECP and contains the same equipment (although the metal detection threshold is lower).

Now, I'll be happy to answer your questions.

**Security Manager Overview:** Good afternoon. I am the Site Security Manager. I'll give you an overview of the site security. You can find more details in your handbook about the site. At the end I'll be happy to answer your questions. First let me tell you some things about our response force:

|   |   |
|---|---|
| <b>Types of Response Force Personnel</b>  | The response force consists of two types of onsite security personnel: <ul style="list-style-type: none"> <li>• Unarmed guards</li> <li>• Armed guards, including tactical response teams</li> </ul>  |
| <b>Responsibilities of Response Force</b> | These security personnel are responsible for: <ul style="list-style-type: none"> <li>• assessment of alarms</li> <li>• administrative duties, such as access control and key service</li> <li>• routine patrol and staffing of fixed posts</li> <li>• response to all security alarms</li> </ul> All posts and patrols have defined policies and procedures with which the guard force must comply.   |
| <b>Supervisors</b>                        | For each shift, one supervisor is present to supervise the guards that conduct administrative duties, patrols, and intrusion alarm response.  |
| <b>Equipment: Unarmed Guards</b>          | All <b>unarmed guards</b> are equipped with: <ul style="list-style-type: none"> <li>• a straight baton</li> <li>• one set of handcuffs</li> <li>• a small flashlight</li> <li>• a handheld radio</li> </ul>   |
| <b>Equipment: Armed Guards</b>            | All <b>armed guards</b> are equipped with: <ul style="list-style-type: none"> <li>• an automatic pistol with a fully loaded magazine</li> <li>• two spare magazines of ammunition</li> <li>• a straight baton</li> <li>• one set of handcuffs</li> <li>• a small flashlight</li> <li>• a handheld radio</li> </ul>  |
| <b>Equipment: Tactical Response Team</b>  | The tactical response team members are equipped with: <ul style="list-style-type: none"> <li>• an automatic pistol with a fully loaded magazine</li> <li>• an automatic assault rifle with a fully loaded magazine</li> <li>• two spare magazines of ammunition for each weapon</li> <li>• a straight baton</li> <li>• handcuffs</li> <li>• flashlight</li> <li>• handheld radio</li> <li>• body armor is readily available in the response force vehicles</li> </ul>   |
| <b>Alarm Stations and Communication</b>   | The <b>Central Alarm Station (CAS)</b> is located in P-1 and is staffed by a minimum of one guard at all times. This guard is responsible for the assessment of alarms and communication to the response force. The security force supervisor is routinely at the CAS.<br>The CAS is equipped with: <ul style="list-style-type: none"> <li>• 100-watt radios that can communicate to all posts and patrols within the boundaries of the Institute</li> <li>• 2 telephone lines—one is linked to each fixed post via a buried telephone cable and the second is a direct link to the offsite response force located in the city</li> </ul> |

|  |  |
|--|--|
|  | All hand-held radios and fixed posts are equipped with a duress switch to allow sending the CAS a covert signal of unauthorized activity. When the CAS receives a duress alarm, the response force is contacted. |
|--|--|

We also have a complete site access control system. The site uses a new badge printing process that prints directly on plastic badge stock. The entire system has changed to this new type of badge, and a background has been designed and a tamper-resistant overlay has been provided for all national sites to use. Although each site has a special alphanumeric identifier that shows where the particular badge was issued, the badges are designed to allow access at all affiliated sites. The badge office (in the Administrative Building outside of the PA) prints all employee and visitor badges for this site. Badge stock is locked up in a safe in the badge office when it is not occupied. Different colors around the border of the badge signify different access authorizations. A legend of these designators is posted in access control points to quickly resolve any questions about access.

Personnel are permitted access through an access control point after verification that they have a current site badge. The guard controlling access is required to verify that the picture matches the badge holder and that the badge has not expired or been revoked. There is an access control office in the Administration Building that issues permanent and temporary badges for access to the plant. There is no check on exiting personnel.

Vehicles authorized routine entry to the site are provided with decals. The security officer(s) on duty permit vehicles to enter upon verifying the vehicle decal and the badges of all vehicle occupants. Temporary vehicle passes may be obtained at the Administration Building with appropriate authorization from site management.

When a delivery vehicle arrives, the guards review the manifest and shipping documents to verify that the truck has a delivery for the institute. The guards then contact the recipient of the delivery to verify that it is expected. Once this is done, the guards inspect the truck for contraband. If the delivery vehicle passes inspection, it is permitted entry to the site. There are no checks on exiting vehicles.

These gates are normally closed and locked with high-security padlocks. When a vehicle arrives, an ECP guard verifies that the driver either has a URF badge permitting access to the URF PA, or has the required escorts. Once the guard has verified that the vehicle is expected, the guard inspects it for contraband. If the vehicle passes inspection, the guards contact the CAS to request that the PA intrusion detection system zone at the gates be placed in the access mode. The guards then unlock the vehicle gates to permit the vehicle entry to the URF PA. After the vehicle has entered the PA, the gates are locked and the PA intrusion detection system zone at the gates is returned to the secure mode.

On exit, vehicles are scanned with a radiation monitor to ensure that there is no contamination and are searched for SNM. Once guards verify that the vehicles are not contaminated and do not have unauthorized SNM, the vehicles are permitted to exit. The contamination scan and SNM search are performed inside the PA with the vehicle gates locked.

Personnel entering the PA undergo a search for contraband by passing through metal and explosive detectors. Hand-carried items are X-rayed and passed through metal detectors. Suspicious items are physically searched. Individuals who fail the metal detector search are either searched again with a hand-held metal detector or subjected to a pat-down search. The personnel then enter the URF PA via a key-card-accessed door. The guards who perform the badge checks have a “panic” button that will override the key card reader, freezing the doors and precluding any entry to the PA. In a Site Emergency, the doors can also be reconfigured to permit egress from the PA to facilitate evacuation. The layout of the entry control section of the URF PA Access Control point is shown in Figure 5.1.

Personnel exiting the PA undergo a search for SNM by passing through metal and SNM detectors. Hand-carried items are X-rayed. Suspicious items are physically searched.

Individuals who fail the metal detector search are either searched again with hand-held metal detectors and SNM detectors or are subjected to a pat-down search. After verification that individuals are not carrying SNM, they undergo a badge exchange, turning in their URF picture badges and key cards and picking up their Site picture badges. The personnel then exit the URF PA via unlocked doors.

The technical unit is also charged with installing locks, making keys, and changing combinations. One master locksmith and several clerks assist with key control. The office for the lock unit is in Administrative Annex 1. All combinations and key blanks are stored in a safe. Records of keys and work requests and completions are kept on a computer in the office. Only the master locksmith and the clerical staff have the password to the system. Keys for office doors, building doors, and padlocks are cut on a special key blank registered to the site. There are not supposed to be any master keys. Once a certain number of keys have been lost (greater than 5%), all locks are re-cored with a new keyway. All combination locks have the combinations changed at least annually. However, if a change in personnel occurs, the combination will be changed immediately.

The URF Site is surrounded by an unalarmed 2.5-meter-high chain-link fence to delineate the legal boundary and keep out trespassers. The URF PA is surrounded by two 2.5-meter-high chain-link fences with an alarmed isolation zone between the two fences. The vital areas within the URF are enclosed by 20-cm-thick reinforced concrete walls with access through 0.75-cm steel-plate water tight doors. Access is controlled by an electronic key card system that releases a door latch. Personnel entering the PA undergo a search for contraband by passing through metal and explosive detectors. Hand-carried items are X-rayed and passed through metal detectors. Suspicious items are physically searched. Individuals who fail the metal detector search are either searched again with a hand-held metal detector or subjected to a pat-down search. The personnel then enter the URF PA via a key-card-accessed door. The guards who perform the badge checks have a “panic” button that will override the key card reader, freezing the doors and precluding any entry to the PA. In a Site Emergency, the doors can also be reconfigured to permit egress from the PA to facilitate evacuation.

In closing, let me add that we have a complete intrusion detection system. The details of this system are identified in your facility handout. Now, do you have any questions?

# Exercise Lecture 2a

## Hypothetical Facility Exercise

---

### Session Objectives:

After the session the participants will:

1. Understand the basic functions of the Hypothetical Facility
2. Identify the different areas of the Hypothetical Facility

### Estimated Time:

25 minutes in subgroups

+25 minutes for large group discussion

50 minutes total

### Exercise:

1. In groups, answer the questions on the Hypothetical Facility.

### Report Your Results in Large Group Discussion:

1. The instructor will share the correct answers with the group. Those groups with differing answers will share their answers and discuss why they chose that answer. The instructor will explain the correct answer.

Exercise 1: in groups, answer the questions below. Be prepared to discuss your answers.

1. How many material Balance Areas are there in the URF? Identify them.
2. What is the through put of the URF?
3. How many lathes are there in the URF processing facility?
4. How many casting furnaces are there in the URF processing facility?
5. Identify the material flow of the URF.
6. Briefly explain the processes that are required to enter the processing floor at the URF.
7. Where is the Analytical Laboratory located?
8. What are the regular working hours of the URF?
9. For a normal test, how long is a part in the X-ray facility?
10. How many storage vaults are located in the processing facility?

11. How many full time employees work at the URF? Of those, how many employees have access to the protected area?

12. What is the community's opinion of the URF?

# Exercise 3a

## Administrative Measures

---

### Session Objectives:

After the session the participants will:

1. Understand the beneficial coexistence between security and safety
2. Understand the mutual benefits between security and material control and accounting elements
3. Understand the complementary nature of other operational activities
4. Understand how effective facility operations reduces theft opportunities for the insider

### Estimated Time:

30 minutes in subgroups  
+ 20 minutes for large group discussion  
50 minutes total

### Exercise:

1. In groups, develop scenarios that identify insider threats and how to mitigate them.
2. Develop an administrative check list of the Technical Demonstration area

### Report Your Results in Large Group Discussion:

1. Each group will present their insider threat. Their partnered group will explain how they diverted the threat.
2. Each group will present their check list and present anomaly resolution actions.

**Exercise 2:** Develop an administrative check list of the Technical Demonstration area

### Instructions:

1. Each group will develop an administrative check table identifying in the table which verification tasks will be performed.
2. Each group will develop actions that should be followed in the event that an anomaly is detected.

Large Group Discussion:

1. Each group will present their check list and present anomaly resolution actions.

# Exercise 3b

## Two-Person Rule

---

### Session Objectives:

After the session the participants will:

1. Know when to apply the two-person rule
2. Understand the requirements for two-person rule participants
3. Recognize locations for two-person rule application
4. Know how to respond to violations

### Estimated Time:

15 minutes in subgroups  
+20 minutes for large group discussion  
35 minutes total

### Exercise:

1. In groups, create a room that requires application of the two-person rule and demonstrate correct and incorrect locations for application of the two-person rule. For incorrect application, the group must report how they would respond to the violation.

### Report Your Results in Large Group Discussion:

1. Each group will present their rooms and demonstrate one correct and one incorrect location for application of the two-person rule. Each group will explain the rationale of their designations for group discussion.
2. Each group will explain how they would respond to the violation of the incorrect placement.

Exercise 1: create a room that requires application of the two-person rule and demonstrate correct and incorrect locations for application of the two-person rule. For incorrect application, the group must report how they would respond to the violation.

**Instructions:**

1. Draw an accurate floor plan for a room that requires application of the two-person rule. (2 drawings will be required).
2. On both floor plans, draw a circle where the work is to be performed. Briefly discuss the operational process that occurs in the room.
3. On one of the floor plans, demonstrate a correct location for the two-person rule team. Explain why this location is correct.
4. On the other floor plan, demonstrate an incorrect location for the two-person rule team. Explain why this location is incorrect.
5. For the incorrect location, explain what response is required for the violation.

Large Group Discussion:

1. Present both floor plans and discuss your rationale for the incorrect and correct locations for the two-person rule team.
2. For the incorrect location, discuss what response is required for the violation

# **Exercise 5a**

## **Technical Measures Checklist**

---

### **Session Objectives:**

**Complete a checklist to help identify all technical measures at entry control points and at target location**

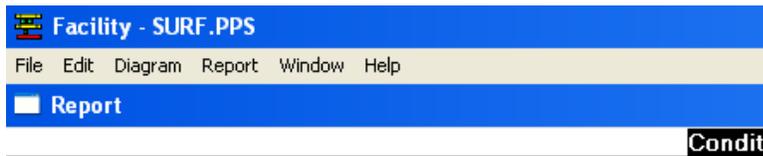
### **Estimated Time:**

**45 minutes**

### **Exercises:**

- 1. Complete checklist as a team**
- 2. Spokesperson for the team briefs the large group on your team's findings**

# Checklist



## SAFEGUARDS

### Access Control

#### Outer

#### ID Check

#### ID Actuated Lock

Pedestrians

Insiders During Evacuation

#### Choice

A Casual recognition

B Credential

C Credential and PIN

D Picture badge

E Picture badge and PIN

F Exchange picture badge

G Exchange picture badge and PIN

H Retinal scan and PIN

I Hand geometry and PIN

J Speech pattern and PIN

K Signature dynamics and PIN

L Fingerprint and PIN

Bypass Key Security -- Stored in controlled location

Note

SAFEGUARDS

Access Control

Contraband Detection

Central

Explosives Detector

Handheld Metal Detector

Portal Metal Detector

Pedestrians

Insiders During Evacuation

Personal Possessions

Packages

Shipments/Cargo

Choice

Tamper Protection - No tamper protection

Maintenance Procedure - No escort required

Testing Procedure - No surveillance

Testing After Maintenance - No independent test

Scheduled Testing Frequency - Less than once each...

Bypass Control - General observation only

Note

X-Ray Inspection

Item Search

Personnel Search

**PASSAGE**

**SAFEGUARDS**

**Access Control**

**Contraband Detection**

**SNM Detection**

**Central**

**Handheld SNM Monitor**

**Portal SNM Monitor**

Pedestrians

Insiders During Evacuation

Personal Possessions

Packages

Tools/Equipment

Shipments/Cargo

**Choice**

Alarm Annunciation - Local only

Tamper Protection - No tamper protection

Maintenance Procedure - No escort required

Testing Procedure - No surveillance

Testing After Maintenance - No independent test

Scheduled Testing Frequency - Less than once each...

Bypass Control - General observation only

Note



**Material Transfer Control**

**Central**

**Transfer Authorization of Target Material**

**Choice**

**A Transfer form check**

**B Signature comparison**

**C Computer verification**

**D Third party verification**

**Timely Completion Confirmation - Not required**

**Note**

**Transfer Procedure for Target Material**

**Verification of Target Material**

**Transfer Authorization of Samples and Sources**

**Transfer Procedure for Samples and Sources**

**Verification of Samples and Sources**

**Transfer Authorization of Other Radioactive Material**

**Transfer Procedure for Other Radioactive Material**

**Verification of Other Radioactive Material**

**Transfer Authorization of Radioactive Waste**

**Transfer Procedure for Radioactive Waste**

**Verification of Radioactive Waste**

**Transfer Carts/Vehicles Inspection**

**Intrusion Detection**

**Outer**

**Exterior Intrusion Sensors**

**Interior Intrusion Sensors**

**Choice**

**A Sonic**

**B Capacitance**

**C Video motion**

**D Infrared**

**E Ultrasonic**

**F Microwave**

**G Multiple noncomplementary sensors**

**H Multiple complementary sensors**

**Tamper Protection - No tamper protection**

**Maintenance Procedure - No escort required**

**Testing Procedure - No surveillance**

**Testing After Maintenance - No independent test**

**Scheduled Testing Frequency - Less than once each...**

**Note**

**Door Penetration Sensor**

**Door Position Monitor**

**Surface Penetration Sensor**

**General Observation**

Security Inspectors

Outer

SI at Post

SI in Tower

SI on Patrol

Central

SI at Post

Choice

A No duress, unprotected

B No duress, small arms protected

C No duress, LAW protected

D No duress, unprotected: small arms prot on alert

E No duress, unprotected: LAW prot on alert

F No duress, small arms protected: LAW prot on alert

G Duress, unprotected

H Duress, small arms protected

I Duress, LAW protected

J Duress, unprotected: small arms prot on alert

K Duress, unprotected: LAW prot on alert

L Duress, small arms protected: LAW prot on alert

Note

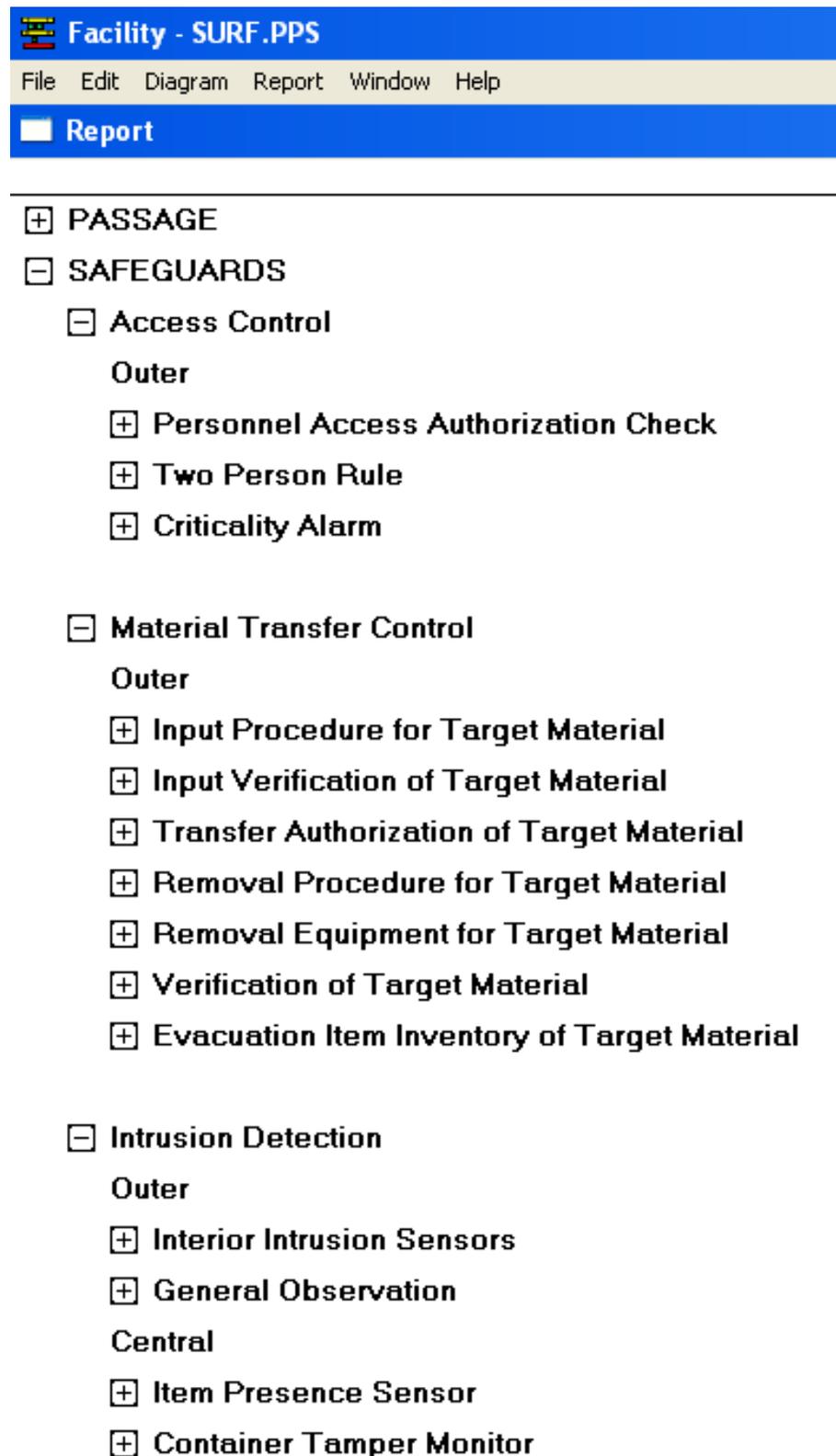
Inner

SI at Post

SI in Tower

SI on Patrol

## Checklist for Target Location:



The image shows a software application window titled "Facility - SURF.PPS". The menu bar includes "File", "Edit", "Diagram", "Report", "Window", and "Help". The "Report" menu is open, displaying a checklist for "Target Location".

- PASSAGE**
- SAFEGUARDS**
  - Access Control**
    - Outer**
      - Personnel Access Authorization Check**
      - Two Person Rule**
      - Criticality Alarm**
  - Material Transfer Control**
    - Outer**
      - Input Procedure for Target Material**
      - Input Verification of Target Material**
      - Transfer Authorization of Target Material**
      - Removal Procedure for Target Material**
      - Removal Equipment for Target Material**
      - Verification of Target Material**
      - Evacuation Item Inventory of Target Material**
  - Intrusion Detection**
    - Outer**
      - Interior Intrusion Sensors**
      - General Observation**
    - Central**
      - Item Presence Sensor**
      - Container Tamper Monitor**



# Exercise 7.1

## Inventory Sampling

---

### Session Objectives:

After the session the participants will be able to do the following:

1. Determine sample size based on various population sizes, goal quantities, and probabilities of defect selection.
2. Determine the Pd from a given inspection plan from a given inventory and sampling plan for a single inventory.
3. Determine the Pd from a given inspection plan from a given inventory and sampling plan over multiple inventories.
4. Apply insider scenario, sampling, and Pd logic to a simulated inventory.

### Estimated Time:

30 minutes in subgroup  
+60 minutes in large group discussion  
90 Minutes total

### Small Group Exercises:

**Materials need:** Computer for each subgroup and Sampling Formula Spreadsheet.

- 1) Determine the sample size for the following situations.
  - a. Goal quantity 2. Probability of Selection 90%. Population size 500
  - b. Goal quantity 3. Probability of Selection 50%. Population size 100
  - c. Goal quantity 1. Probability of Selection 95%. Population size 100
- 2) For 1a, 1b, and 1c determine how many inventories it takes for the probability of detection to reach .999. Assume if the defective item is selected the Pd = 1.
- 3) Based on a given insider scenarios and inventory procedure, identify the associated probability of detection.

### Large Group Exercise:

- 4) Review correct answers to problems from small group breakout session.
- 5) Play inventory sampling game using population of 100 items.

### **Exercise 3-1 – Use the Population from 1b**

**Insider Scenario** – insider has stolen a single container of material.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location. No confirmatory or verification measurements are made.

What is the probability of detecting the missing item?

How many inventory periods does it take for the probability to be greater than 99%?

### **Exercise 3-2 - Use the Population from 1b**

**Insider Scenario** – insider has removed 100 grams of material from a single item. The insider was successful in defeating the TID and other safeguards so the item appears normal to a visual inspection.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location.

What is the probability of detecting the defect in the item?

How many inventories does it take for the probability to be greater than 99%?

### **Exercise 3-3 - Use the Population from 1b**

**Insider Scenario** – insider has removed 100 grams of material from a single item. The insider was successful in defeating the TID and other safeguards so the item appears normal to a visual inspection.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location. A confirmatory weight measurement is made on a random sample of the inventory.

What is the probability of detecting the defect in the item?

How many inventories does it take for the probability to be greater than 99%?

### **Exercise 3-4 - Use the Population from 1b**

**Insider Scenario** – insider has removed 100 grams of material from a single item and substituted inert material weighing 100 grams. The insider was successful in defeating the TID and other safeguards so the item appears normal to a visual inspection.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location. A confirmatory weight measurement is made on a random sample of the inventory.

What is the probability of detecting the defect in the item?

How many inventories does it take for the probability to be greater than 99%?

### **Exercise 3-5 - Use the Population from 1b**

**Insider Scenario** – insider has removed 100 grams of material from a single item and substituted inert material weighing 100 grams. The insider was successful in defeating the TID and other safeguards so the item appears normal to a visual inspection.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location. A verification measurement is made on a random sample of the inventory.

What is the probability of detecting the defect in the item?

How many inventories does it take for the probability to be greater than 99%?

## **Exercise 5 – Large Group**

### **Materials Needed –**

- 1) Inventory of 100 small containers (preferably small transparent prescription bottles) serialized 1-100. Inside 85 containers place 2 normal jelly beans. Inside 5 containers place only 1 jelly bean. Inside 5 containers place 1 normal jelly bean and 1 “vomit (e.g., Harry Potter Jelly Bean)” flavored jelly.
- 2) Inventory sampling spreadsheet to determine random sample.

### **Instructions:**

- 1) Develop a sampling plan based on 90% probability of selecting a defective item.
- 2) Demonstrate each scenario in section 3 (3-1, 3-2, 3-3, 3-4, and 3-5).
  - a. For missing item or 3-1 remove one container from the population.
  - b. The 5 items with one jelly bean missing should be considered the items where the insider has reduced the weight by 100 grams. Weighing can be done but a visual of the container contents can be used to simulate the confirmatory measurement.
  - c. For 3-5 or verification measurement, the method of verification measurement will be destructive analysis (e.g., eat the jelly beans to determine if they’re good or vomit flavored).

Review Pd of detection and the relationship to goal quantity, insider scenario, and method of inspection.

$n = (N-d) / (1 - \beta^{1/(d+1)})$

N Population Size  
 β is the specified probability of failing to find at least one critical nonconformity  
 d is the maximum number of criticality non-conforming items "allowed" in the lot. Goal Quantity.

n Sample Size

| Goal Quantity = d items and chance of finding at least one defect x% |   |      |                  |
|--|---|------|------------------|
| N  | d | β    | n or sample size |
| 500  | 2 | 0.1  | 267              |
| 100  | 3 | 0.5  | 16               |
| 100  | 1 | 0.05 | 77               |
| 100  | 1 | 0.05 | 77               |

# Exercise 7.4

## Trickle Diversion Exercise with Process Control

---

### Session Objectives:

After the session the participants will be able to do the following:

1. Prepare Shewart, CUSUM, and EWMA charts for sample ID data.
2. Estimate the Pd point in time for various inside trickle diversion rates.

### Estimated Time:

1.5 hours in subgroup  
+1.0 hour in large group discussion  
2.0 hours total

### Small Group Exercises:

**Materials need:** Computer for each subgroup with Bulk Exercise Spreadsheet, Excel, and QI Macros for Excel Version 2008.10.

- 1) Using the sample data introduce a 1.75 kg insider trickle diversion per month from months 25 – 34. Prepare a Shewart, CUSUM, and EWMA chart for the data.
  - a. Do any of the 3 analysis methods indicate an out of control situation? Under WECO rules?
  - b. Do any of the 3 analysis methods indicate a process shift?
- 2) Using the sample data introduce a 2.0 kg insider trickle diversion per month from months 25 – 34. Prepare a Shewart, CUSUM, and EWMA chart for the data.
  - a. Do any of the 3 analysis methods indicate an out of control situation? Under WECO rules?
  - b. Do any of the 3 analysis methods indicate a process shift?
- 3) Using the sample data introduce a 1.75 kg insider trickle diversion every other month from months 25 – 34. Prepare a Shewart, CUSUM, and EWMA chart for the data.
  - a. Do any of the 3 analysis methods indicate an out of control situation? Under WECO rules?
  - b. Do any of the 3 analysis methods indicate a process shift?
- 4) Using the sample data introduce a 10 gram insider trickle diversion per month from months 25 – 34. Prepare a Shewart, CUSUM, and EWMA chart for the data.
  - a. Do any of the 3 analysis methods indicate an out of control situation? Under WECO rules?
  - b. Do any of the 3 analysis methods indicate a process shift?

## **Large Group Exercise:**

- 5) Review control charts for each of the 4 possible scenarios
- 6) Discuss possible insider strategies with respect to rates
- 7) Discuss the following questions?
  - a. You were given the statistical limits that apply to this process based on its current design. How does that relate to specification or safeguards limits?
  - b. What are the next steps to consider with respect to improving the process?

### **Exercise 3-1 – Use the Population from 1b**

**Insider Scenario** – insider has stolen a single container of material.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location. No confirmatory or verification measurements are made.

What is the probability of detecting the missing item?

How many inventory periods does it take for the probability to be greater than 99%?

### **Exercise 3-2 - Use the Population from 1b**

**Insider Scenario** – insider has removed 100 grams of material from a single item. The insider was successful in defeating the TID and other safeguards so the item appears normal to a visual inspection.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location.

What is the probability of detecting the defect in the item?

How many inventories does it take for the probability to be greater than 99%?

### **Exercise 3-3 - Use the Population from 1b**

**Insider Scenario** – insider has removed 100 grams of material from a single item. The insider was successful in defeating the TID and other safeguards so the item appears normal to a visual inspection.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location. A confirmatory weight measurement is made on a random sample of the inventory.

What is the probability of detecting the defect in the item?

How many inventories does it take for the probability to be greater than 99%?

### **Exercise 3-4 - Use the Population from 1b**

**Insider Scenario** – insider has removed 100 grams of material from a single item and substituted inert material weighing 100 grams. The insider was successful in defeating the TID and other safeguards so the item appears normal to a visual inspection.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location. A confirmatory weight measurement is made on a random sample of the inventory.

What is the probability of detecting the defect in the item?

How many inventories does it take for the probability to be greater than 99%?

### **Exercise 3-5 - Use the Population from 1b**

**Insider Scenario** – insider has removed 100 grams of material from a single item and substituted inert material weighing 100 grams. The insider was successful in defeating the TID and other safeguards so the item appears normal to a visual inspection.

**Inventory Procedure** – 100% of the inventory is verified by serial number, TID, and location. A verification measurement is made on a random sample of the inventory.

What is the probability of detecting the defect in the item?

How many inventories does it take for the probability to be greater than 99%?

## **Exercise 5 – Large Group**

### **Materials Needed –**

- 1) Inventory of 100 small containers (preferably small transparent prescription bottles) serialized 1-100. Inside 85 containers place 2 normal jelly beans. Inside 5 containers place only 1 jelly bean. Inside 5 containers place 1 normal jelly bean and 1 “vomit (e.g., Harry Potter Jelly Bean)” flavored jelly.
- 2) Inventory sampling spreadsheet to determine random sample.

### **Instructions:**

- 1) Develop a sampling plan based on 90% probability of selecting a defective item.
- 2) Demonstrate each scenario in section 3 (3-1, 3-2, 3-3, 3-4, and 3-5).
  - a. For missing item or 3-1 remove one container from the population.
  - b. The 5 items with one jelly bean missing should be considered the items where the insider has reduced the weight by 100 grams. Weighing can be done but a visual of the container contents can be used to simulate the confirmatory measurement.
  - c. For 3-5 or verification measurement, the method of verification measurement will be destructive analysis (e.g., eat the jelly beans to determine if they’re good or vomit flavored).

Review Pd of detection and the relationship to goal quantity, insider scenario, and method of inspection.

# Exercise 8

## Target Analysis

---

### Session Objectives:

After the session the participants will be able to do the following:

1. Understand the basic steps of target identification
2. Describe the URF targets in detail
3. Characterize specific targets with more detail
4. Prioritize targets based on DOE guidance documents
5. Understand the graded safeguards concept
6. Identify roll up and understand why it is a concern
7. Recognize the Category and Attractiveness levels for different materials

### Estimated Time:

60 minutes in subgroups  
+30 minutes in large group discussion  
90 minutes total

### Exercises:

1. Read the detailed URF site information on targets and target locations and fill out the Target Characterization Worksheet for your subgroup's assigned target.
2. Determine if roll up is credible in a particular area of the URF using the question that identify roll up. Once roll up is determined, use the DOE Characterization of Nuclear Material Chart to determine what attractiveness and category the material rolls up to.

**Attachment: DOE Graded Safeguards Table**

**Exercise 1: Read the detailed URF site information on targets and target locations and fill out the Target Characterization Worksheet for your subgroup's assigned target.**

**Instructions:**

1. Read the detailed URF site information on targets and target locations.
2. Based on the detailed target information you have been provided and your assigned target, complete the Target Characterization Worksheet below with as much information as possible (your team may have to make some assumptions). Any incomplete areas will help to identify what additional information still needs to be collected.

**Materials in Bunker**

The uranium in the bunker consists of materials received for recycling or finished products packed and ready to ship. The material for recycling is on open shelves inside the bunker. Received material is in approved shipping containers. The received containers weigh 100 kg. The containers consist of a heavy gauge steel drum with a bolt on lid. The lid is held by six bolts and after being tightened down to a specified bolt tension, each bolt has a TID run through it to indicate if any tampering has occurred. Inside the steel shipping container is the material container. A packing sleeve is placed in the shipping container to secure the material container. Then the material container is placed in the shipping container and another packing sleeve is placed in the shipping container to secure the material container. The material container is a heavy gauge steel container with a lid secured by six bolts. This container is also sealed with a TID on one bolt. The shipping container weighs 65 kg, the packing material weighs 7 kg, the material container weighs 25 kg and the material weight is between 2 and 3 kg.

The product containers are inside an expanded metal locked enclosure and weigh 50 to 100 kg (depending on the type). The 100 kg product containers are essentially the same as the containers for received material. The 50 kg containers are designed to fit inside a larger shipping overpack container and are not as robust as the 100 kg container. They are about one half as tall and the lids snap on with three quick release levers. The same type of inner container is used for all items (there will be some variations in shape/size).

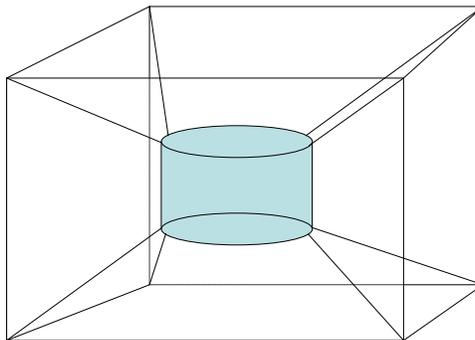
**Materials in Processing Building Vaults**

The material in the processing building vaults is in various forms and quantities:

- The chip vault has material in all sizes, shapes and enrichments. When parts to be recycled come to the facility, they are crushed into small chips (between 200 and 500 grams each normally). These chips are classified by enrichment and stored in 2 liter stainless drawers. The amount of material in each can may vary, but nuclear safety has established a limit of 1 kg of material in each drawer regardless of the enrichment. These cans are stored on open shelves in the vault. When an ingot is needed for machining, and there is not one available meeting requirements in the billet vault, a batch of chips and powder is put together that matches the requirements. This is done in

the makeup area directly outside of the chip vault. A technician takes chips from various drawers in the vault or uses  $UO_2$  powder to make up a batch.

- The billet vault contains 5 kg billets. When new parts are to be manufactured, chips are consolidated in a lot and brought to the casting line, here they are melted and poured into a mold for a billet. The billets (after a cooling period) are collected and stored in plastic bags inside metal cans. These metal cans are an integral part of the birdcages (see figure 1). The birdcages ensure correct separation distances and add some delay to the material. Each birdcage weighs 20 kg and is stored on the floor or on open shelves.
- The product vault contains the finished parts before they are shipped. These parts are stored in a special birdcage insider an inert gas package. The birdcage is essentially the same as the billet birdcage with a different container integrated into it. The finished products normally weigh between 2 and 3 kg (depending on the particular product being manufactured). The birdcage weighs 20 kg and is stored inside an expanded metal enclosure within the vault.



**Figure 1. Birdcage**

### **Materials in Processing Area**

The amount of material exposed in the processing area at any one time in the material process can range from 6 to 50 kg but is only present during the normal five day work period. The bird cages with the material for specific machine input and output are moved by cart to the machine area at the start of each shift and are locked in place to a ring set in the floor. The material handlers have the key to lock the birdcage to the floor. The machinist has the key to open the cage to mount the material in the machine. Mounting the material can take 30 minutes, but dismounting can be done in 15 seconds. Since mounting takes so long on some machines, during breaks the material is left in the machine. When the machining is done, the product is put back in the birdcage and stored until it is picked up on pickup rounds. The material custodian has a schedule of work and picks up the product soon after it is completed. If there is a problem in the process and the product will not be ready for pickup on schedule, the machinist notifies his

supervisor who notifies the Material Custodian. Material at various stages of machining is stored in the billet vault during the non-working hours.

### **Materials moved from the Processing Area**

When a product is complete it is moved to the quality control area where it is inspected. This area is set up as a vault since some materials may stay here for extended periods of time. Products will also be sent via inter-site convoy to the x-ray facility as part of quality control. Once material has passed quality control, it is packed in the material container and stored in the product vault. In preparation for off-site shipment, products are packaged in shipping containers and moved to the bunker for storage pending shipment. Material is shipped out on schedule set by the military.

### **Materials in Basement Recovery Area**

Material is also accumulated in the recovery area in the basement. The turnings from the machines that are taken up in the cooling fluid are stored in the recovery area until a significant amount has accumulated. When weight differences indicate that greater than 2 kg of material is in the recovery area, recovery operations are undertaken, the fluid is filtered away from the material in a settling tank. When the fluid has been drawn away, the filter material is washed to recover the Uranium. The recovered uranium is weighed, put in a can and sent back up to the chip vault for later re-use. A sample of the material will be taken and sent to the analytical lab to determine the isotopic content of the material (since many different enrichments may be machined in one batch)

### **X-ray Facility**

Parts are in the X-ray for about 6 hours during a normal test. When things are not normal (e.g. when there are potential problems that need more investigation), parts can be left there overnight (to preserve the diagnostic setup). When materials are in the X-ray facility overnight, patrols put a seal on the door and check the seal every 30 minutes. The X-ray facility is constructed like a vault. When material is left there it is left in a positioning unit that it can be removed from in 60 seconds.

### **Shipping and Receiving Warehouse**

Shipments are put into the vault the same day they are received, but are often left in the shipping and receiving warehouse for 2 to 3 hours while the receiving paperwork is completed and all the weights and serial numbers are verified. While in the shipping and receiving warehouse, material is constantly attended and Patrols check on them every 30 minutes. Material in these locations will be in the 100 kg shipping containers that they will be stored in until put into the recycling process.

### **Analytical Laboratory**

The analytical laboratory is situated between Technical Area Administrative Annex I and II. The first floor of the analytical laboratory is alarmed with a balanced magnetic switch (BMS) sensor on the door and passive infrared (PIR) sensors, providing interior volumetric intrusion detection. The windows also have iron bars across them. Transfers of samples to the Analytical Laboratory

and waste to the Waste Measurement Facility are handled by Operations Support Personnel. Since these are Category III/IV quantities, the two person rule is not applied.

### **Material Waste**

Nuclear material in the form of waste is generated from various parts of the process. Waste is collected and placed in waste receptacles. On a regular schedule, the operation support personnel collect and package the waste into waste containers. Once packaged, this material is moved on a bi-weekly basis to the Waste Measurement Facility where it is assayed and the nuclear content determined. Once assay is completed, the waste packages are transferred to the shipping receiving facility to await transport for burial.

| <b>Target Characterization Worksheet</b> |                    |                         |
|--|--------------------|-------------------------|
| <b>Target:</b>                           |                    | <b>Target Location:</b> |
|  | <b>Description</b> | <b>Comments</b>         |
| <b>Material Form</b>                     |                    |                         |
| <b>Attractiveness Level</b>              |                    |                         |
| <b>Category</b>                          |                    |                         |
| <b>Container Characteristics</b>         |                    |                         |
| <b>Restraints</b>                        |                    |                         |
| <b>Weight</b>                            |                    |                         |
| <b>Portability</b>                       |                    |                         |
| <b>Radiation Level</b>                   |                    |                         |
| <b>Discrete or Roll-up</b>               |                    |                         |
| <b>Other:</b>                            |                    |                         |

**Exercise 2: determine if roll up is credible in a particular area of the URF using the questions that identify roll up. Once roll up is determined, use the DOE Attractiveness and Categorization Chart to determine what category the material rolls up to.**

**Instructions:**

1. Using the guideline questions for roll up credibility, determine what amount of roll-up there is for your facility/areas.
2. Using the DOE Categorization of Material Chart, determine what category the material rolls up to.

**Large Group Discussion:**

1. Each group will present their findings to the group explaining how they determined the level of roll up.
2. Each group will explain what category they assigned to the roll up material.

Group 1:

Location and amount of material:

| <b>Location</b>       | <b>Amount</b>   |
|-----------------------|---|
| Product Bunker        | 5 containers, 1.75 kg each oxide (Attractiveness level "C")   |
| Analytical Laboratory | 200 samples, .5 g each oxide (Attractiveness level "C");<br>100 samples (.25 liter) 35g/liter (Attractiveness level "C"); |
| X-ray Facility        | 2 kg metal (Attractiveness level "B")   |

- Materials outside of MAAs
  - Is the total amount of SNM greater than a goal quantity? \_\_\_\_\_
  - Can the Insiders gain access to enough areas to accumulate a goal quantity at a point in time? \_\_\_\_\_
  - Can the Insiders credibly accumulate a goal quantity before detection (or with a relatively lower probability of detection)? \_\_\_\_\_
- Materials within an MAA
  - Are lesser attractive materials treated differently? \_\_\_\_\_
  - Can Insiders accumulate a goal quantity before detection (or with a relatively lower probability of detection)? \_\_\_\_\_
  - Can Insiders divert, hide, and accumulate the material undetected prior to removal? \_\_\_\_\_

**Is roll up credible?** \_\_\_\_\_

**What category does the material roll up to?** \_\_\_\_\_

Group 2:

Location and amount of material:

| <b>Location</b>        | <b>Amount</b>  |
|------------------------|--|
| Chemical Make-up Area  | 20 drawers; each drawer contains 250g oxide (Attractiveness level "C") |
| Basement Recovery Area | 900 grams metal (Attractiveness level "B")                             |
| Billet Vault           | 2 billets containing 5 kg ingots (Attractiveness level "B")            |

- Materials outside of MAAs
  - Is the total amount of SNM greater than a goal quantity? \_\_\_\_\_
  - Can the Insiders gain access to enough areas to accumulate a goal quantity at a point in time? \_\_\_\_\_
  - Can the Insiders credibly accumulate a goal quantity before detection (or with a relatively lower probability of detection)? \_\_\_\_\_
- Materials within an MAA
  - Are lesser attractive materials treated differently? \_\_\_\_\_
  - Can Insiders accumulate a goal quantity before detection (or with a relatively lower probability of detection)? \_\_\_\_\_
  - Can Insiders divert, hide, and accumulate the material undetected prior to removal? \_\_\_\_\_

**Is roll up credible?** \_\_\_\_\_

**What category does the material roll up to?** \_\_\_\_\_

Group 3:

Location and amount of material:

| <b>Location</b>       | <b>Amount</b>   |
|-----------------------|---|
| Product Bunker        | 1 container with 1.5 kg oxide (Attractiveness level "C") each   |
| Analytical Laboratory | 100 samples, .5g each oxide; 100 (.25 liter) samples 25g/liter; |
| X-ray Facility        | 2 kg metal (Attractiveness level "B")                           |

- Materials outside of MAAs
  - Is the total amount of SNM greater than a goal quantity? \_\_\_\_\_
  - Can the Insiders gain access to enough areas to accumulate a goal quantity at a point in time? \_\_\_\_\_
  - Can the Insiders credibly accumulate a goal quantity before detection (or with a relatively lower probability of detection)? \_\_\_\_\_
- Materials within an MAA
  - Are lesser attractive materials treated differently? \_\_\_\_\_
  - Can Insiders accumulate a goal quantity before detection (or with a relatively lower probability of detection)? \_\_\_\_\_
  - Can Insiders divert, hide, and accumulate the material undetected prior to removal? \_\_\_\_\_

**Is roll up credible?** \_\_\_\_\_

**What category does the material roll up to?** \_\_\_\_\_

Group 4:

Location and amount of material:

| <b>Location</b>        | <b>Amount</b>  |
|------------------------|--|
| Casting Furnace Area   | 3 kg oxide<br>(Attractiveness level<br>"C");                   |
| Waste Receptacles      | 5 receptacles 200g/each<br>oxide (Attractiveness<br>level "C") |
| Basement Recovery Area | 199 grams<br>(Attractiveness level<br>"B")                     |

- Materials outside of MAAs
  - Is the total amount of SNM greater than a goal quantity? \_\_\_\_\_
  - Can the Insiders gain access to enough areas to accumulate a goal quantity at a point in time? \_\_\_\_\_
  - Can the Insiders credibly accumulate a goal quantity before detection (or with a relatively lower probability of detection)? \_\_\_\_\_
- Materials within an MAA
  - Are lesser attractive materials treated differently? \_\_\_\_\_
  - Can Insiders accumulate a goal quantity before detection (or with a relatively lower probability of detection)? \_\_\_\_\_
  - Can Insiders divert, hide, and accumulate the material undetected prior to removal? \_\_\_\_\_

**Is roll up credible?** \_\_\_\_\_

**What category does the material roll up to?** \_\_\_\_\_

**What level of protection would be allocated to this category?** \_\_\_\_\_

# Exercise 6

## Insider Threat Group Table for Targets

---

### Session Objectives:

After the session the participants will be able to do the following:

1. Gather information on potential insiders based on job functions.
2. Generate threat group tables for targets
3. Prioritize insider threat groups

### Estimated Time:

30 minutes in subgroups  
+20 minutes for large group discussion  
50 minutes total

### Exercises:

1. Develop a Threat Group Table that defines qualitatively (high, medium, and low) the level of access, authority, and knowledge that each insider has for one of the following theft targets: (Each group will be assigned one target.)
  - The X-Ray facility
  - The machining area during day shift
  - The chip vault during night shift
  - The casting furnace area
2. Prioritize the five positions for your theft target.

### Report Your Results in Large Group Discussion:

1. Each subgroup will present their qualitative designations for access, authority, and knowledge for their assigned theft target. Each group will explain the rationale of their designations for group discussion.
2. Each subgroup will present their ranking for group discussion.

Exercise 1: Develop a Threat Group Table

**Instructions:** Using the blank Threat Group Table, assign a designation (high, medium, or low) for the level of access, authority, and knowledge for each job position for your assigned theft target.

- Step 1. Use the URF Staffing Table to identify relevant job positions for your theft target.
- Step 2. Identify a descriptor for each insider attribute (access, authority, and knowledge) for each job position.
- Step 3. Assign a designator (high, medium, or low) for the level of access, authority, and knowledge for your assigned theft target.

Example:

## Example of H,M,L Applied to Threat Group Table for the Bunker

| Position (Number)  | Routine Access   | Routine Authority / Responsibility  | Knowledge  |
|--|--|---|--|
| Plant Manager (1)<br>(Plant Manager Org.)  | Protected Area, All Inner Areas (usually escorted) <b>L</b>                        | Overall direction. Not authorized to direct detailed facility operations <b>M</b>                           | General knowledge of plant operations, lacks detailed understanding of facility <b>M</b>               |
| Shift Supervisor (3 total with 1 per shift)<br>(Shift Supervisor Org.)                     | Protected Area, All Inner Areas <b>L</b>   | Detailed direction of all facility activities. Directly obeyed without question in most situations <b>H</b> | Extensive, detailed knowledge about all aspects of facility design, layout, and operation. <b>M</b>    |
| Machining operator (6 total with nominal 4 per day shift)<br>(Operations Support Org.)     | Protected Area, All Inner Areas <b>L</b>   | Detailed direction of all machining activities. Under direction of shift supervisor. <b>L</b>               | Extensive, detailed knowledge about all activities in the machining area. <b>M</b>                     |
| Health Physics Technicians (4 total with nominal 3 per day shift)<br>(Health Physics Org.) | Protected Area, all Inner Areas and occasional escorted access to Storage <b>M</b> | Monitor radiological conditions. Not permitted to work on plant equipment. <b>L</b>                         | Specialized knowledge related to their duties. Narrow knowledge of facility systems. <b>M</b>          |
| Operations Support (6 total with nominal 4 per day shift)<br>(Operations Support Org.)     | Protected Area, All Inner Areas and occasional escorted access to Storage <b>M</b> | Perform specific operations tasks under direction of machining and casting operators <b>L</b>               | Specialized knowledge related to their duties. Narrow knowledge of complete facility systems. <b>M</b> |

September 2007

24

# Exercise 1

## Threat Group Table for \_\_\_\_\_

| Position (Number) | Routine Access | Routine Authority / Responsibility | Knowledge |
|-------------------|----------------|------------------------------------|-----------|
|                   |                |                                    |           |
|                   |                |                                    |           |
|                   |                |                                    |           |
|                   |                |                                    |           |
|                   |                |                                    |           |

**Exercise 2:** Rank the Five Positions for your theft target.

**Instructions:** Using the completed Threat Group Table for your theft target, rank the five positions from highest degree of access to lowest degree of access

Example: Degree of Access for the Bunker

| Ranking | Position                  | Routine Access | Routine Authority/Responsibility | Knowledge |
|---------|---------------------------|----------------|----------------------------------|-----------|
| 1       | Health Physics Technician | M              | L                                | M         |
| 2       | Operations Support        | M              | L                                | M         |
| 3       | Shift Supervisor          | L              | H                                | M         |
| 4       | Plant Manager             | L              | M                                | M         |
| 5       | Machining Operator        | L              | L                                | M         |

**Degree of Access for \_\_\_\_\_**

| Ranking | Position | Routing Access | Routing Authority/Responsibility | Knowledge |
|---------|----------|----------------|----------------------------------|-----------|
| 1       |          |                |                                  |           |
| 2       |          |                |                                  |           |
| 3       |          |                |                                  |           |
| 4       |          |                |                                  |           |
| 5       |          |                |                                  |           |

# Exercise 10 Case Studies

---

## Session Objectives:

After the session the participants will be able to do the following:

1. Identify or speculate insider motivations for each case study.
2. Identify or speculate which MPC&A elements were defeated or circumvented.

## Estimated Time:

1.0 hours in subgroup  
+0.5 hour in large group discussion  
1.5 hours total

## Small Group Exercises:

**Materials need:** None

## Instructions:

- 1) For each case study the participants and facilitator will read through the case study and identify the following:
  - a. Insider motivations
  - b. MPC&A elements defeated or bypassed during the theft

## Case Study 1 – General Electric LEU Plant in Wilmington NC USA

On Friday, January 26, 1979, a temporary employee of a subcontractor working at the General Electric low enriched fuel fabrication plant in Wilmington North Carolina stole two 5-gallon containers of low enriched  $UO_2$  (145 pounds total). The theft was accomplished as follows. After working the day shift, he drove back to the plant at 10:50 P.M. and entered with the night shift. He circumvented the access controls at the entrance gate by showing the guard his Florida driver's license which looked similar to a picture badge authorizing access to the plant area where the  $UO_2$  was processed. His yellow contractor badge would not have permitted access to this area. He had allegedly used his driver's license to gain access to this area on previous occasions. Once inside the plant, the subject would have been guided by gates and fences into a parking area had it not been for the fact that one gate had been removed to allow installation of truck scales. The missing gate made it possible for him to drive to an area adjacent to the building he wanted to enter and park his car. He entered the building and went to his normal work station, the Chem Tech Lab, entering it using his key. In the lab he picked up his protective clothing, a two wheel cart used to move 55 gallon drums, and a container used to ship chemicals. The container could hold two 5-gallon cans. He then proceeded to a door leading up a stairwell into the radiation controlled area. The door was normally locked (though there was no regulatory requirement to do so). However, at this time it was slightly ajar due to malfunction of the locking mechanism. Once through the door, he put on his protective clothing and went up the stairs to the Blend Queue Area. He removed two 5-gallon cans of  $UO_2$ , carried them down the stairs and put them in the shipping container. He then removed his protective clothing and retraced his steps back to his workstation, the Chem Tech Lab.

Once back in the lab he opened one can and removed some of the material, which he intended to use to effect his blackmail scheme. Using the 2 wheel cart, he transported the remaining material to his car and loaded it into his trunk. He retraced his steps and left the plant just before midnight on Friday, January 26. (Plant procedures required anyone leaving the plant after midnight to sign out.) He had been in the plant approximately one hour. He had entered the plant with the incoming plant change and had left with the outgoing shift.

At 11:45 AM. on the following Monday, January 29, the plant General Manager reported to authorities that he had found an extortion letter and a sample of  $UO_2$  at his door when he came to work. The letter stated that the writer had taken two 5-gallon containers of  $UO_2$  from the plant and identified the containers by serial number and gross weight. The letter also stated that sufficient  $UO_2$ , had been removed from one of the containers to furnish samples to newspaper editors, senators, anti-nuclear group leaders, and others, if his demand for \$100,000 in cash was not met by Thursday, February 1. The writer further threatened that, after the samples had been delivered, if he had not received the money, one container of  $UO_2$  would be dispersed through one unnamed large American city. The  $UO_2$  powder from the second container would be dispersed through another large city if an additional \$100,000 was not provided at that time.

As the General Manager was in the process of verifying the authenticity of the container numbers and determining whether they were missing, he received independent notification from the plant's near real time accounting system that the two containers were not in their assigned locations and could not be accounted for. The Federal Bureau of Investigation (FBI) assumed

investigative jurisdiction on January 29 and arrested the perpetrator on February 1, 1979. The perpetrator, a temporary employee, was subsequently convicted and sentenced to 15 years in prison. (From IE Circular No. 79-08, "Attempted Extortion - Low Enriched Uranium", May 17, 1979.)

- 1) What was the speculated insider motivation?
- 2) What technical measures were defeated? How?
- 3) What administrative measures were defeated? How?

### **Case Study 2 – Ignalina Nuclear Power Plant, Ignalina Lithuania**

August 1992, a 7-meter long fuel assembly weighing 270 kg and containing 111 kg of 2% enriched LEU was stolen from the Ignalina Nuclear Power Plant, in Ignalina, Lithuania. It was removed from the facility by attaching it to the bottom of a duty bus. The investigation revealed that the reactor operation personnel and the guards had carried out the theft. About 80 kg of the stolen LEU are said to have been recovered on several occasions between 1992 and 2002. (Presentation by Chaim Braun, Fritz Steinhausler, Lyudmila Zaitseva at the ANS 2002 Winter Meeting).

- 1) What was the speculated insider motivation?
- 2) What technical measures were defeated? How?
- 3) What administrative measures were defeated? How?

### **Case Study 3 – Chepetsk Plant, Lzhevsk Russia.**

In 1992, Russian security agents detained a group of criminals who had been stealing Uranium from the Chepetsk plant in Lzhevsk and seized 140 kg of LEU (2% to 4% enrichment). Facility employees stole the material taking advantage of an accounting system weakness that allowed a 4% "loss of inventory" in material balance closures. Based on the incident, an inventory was conducted at the plant and 300 kg were found to be missing. Portions of the diverted material are believed to have been seized in Poland, Belarus, Lithuania, Russia, and Chechnya between 1992 and 2002. (Presentation by Chaim Braun, Fritz Steinhausler, Lyudmila Zaitseva at the ANS 2002 Winter Meeting)

- 1) What was the speculated insider motivation?
- 2) What technical measures were defeated? How?
- 3) What administrative measures were defeated? How?

#### **Case Study 4 – Luch Scientific Production Association, Podolsk Russia**

The first confirmed case involving the diversion of fissile material from nuclear materials in the former Soviet Union occurred at the Luch Scientific Production Association in Podolsk, a town approximately 40 kilometers southwest of Moscow. Between late May and early September 1992, Leonid Smirnov, a chemical engineer and long-time employee of the plant, stole approximately 1.5 kg of weapons-grade uranium. He accumulated this quantity by some 20-25 difference diversions, taking the material in the form of UO<sub>2</sub> powder from the facility in glass jars and storing it on his apartment balcony.

Smirnov had no accomplices and appears to have been motivated by an article he read in a Russian newspaper about the fortune to be made by selling HEU. He was apprehended at the Podolsk Railroad Terminal on October 9, 1992 along with most of the HEU concealed in 3 lead cylinders. He had planned to travel to Moscow for the purpose of selling the nuclear material. Although Smirnov initially confessed to having a specific customer from the Caucasus in mind, the official investigation concluded there was no concrete buyer who had been contacted.

- 1) What was the speculated insider motivation?
- 2) What technical measures were defeated? How?
- 3) What administrative measures were defeated? How?

#### **Case Study 5 – Northern Fleet Naval Base, Andreeva Guba, Russia**

One of the earlier confirmed thefts of HEU occurred in late July 1992 at a storage facility of the Northern Fleet naval base at Andreeva Guba, 40 kilometers from the Norwegian border. Two naval servicemen were arrested in the case and accused of stealing 1.8 kg of HEU from two fuel assemblies. The material, which was recovered, was enriched to 36% and used as fuel for 3<sup>rd</sup> generation naval reactors. The men said they were operating under the instructions from two naval officers – both of whom denied involvement in the theft. At the trial of the four suspects, which concluded in November 1995, the two naval servicemen were sentenced to prison terms of 5 years. The two naval officers were found not guilty due to lack of evidence. Additional suspects associated with a Murmansk – St. Petersburg criminal ring are still under investigation.

- 1) What was the speculated insider motivation?
- 2) What technical measures were defeated? How?
- 3) What administrative measures were defeated? How?

## **Case Study 6 – Mound Laboratory, Miamisburg, OH USA**

In the late 70's a small Pu238 source was discovered missing from a storage vault during a routine monthly inventory. During the previous month inventory the source had been successfully inventoried. The only access to the vault had been by authorized operations personal and the custodial staff. Although an investigation occurred the source was not located and questioning of personnel did not reveal any information. In the late 1980's as the building was being decommissioned the source was found in the drain trap of the "mop" closet sink (e.g., closet where custodial and cleaning supplies are stored and mop buckets emptied).

Even though it was speculated the source might have been in the drain the entire time. Perhaps it had somehow accidentally or purposely fallen into the mop bucket while the vault was being cleaned. It wasn't discovered earlier because background radiation from the process perhaps prevented measurement sweeps from seeing the source. It was only during decommissioning where the process was being dismantled and radiation levels were lower that allowed the source to be detected.

- 1) What was the speculated insider motivation?
- 2) What technical measures were defeated? How?
- 3) What administrative measures were defeated? How?

# Exercise 12

## Abrupt Theft Analysis

---

### Session Objectives:

After the session the participants will be able to do the following:

1. Identify alternative actions and strategies that an insider could use during each step of an abrupt theft scenario
2. Identify protection measures that might detect each insider action
3. Qualitatively evaluate the effectiveness of each protection measure for each insider action
4. Identify the best insider scenario

### Estimated Time:

60 minutes in subgroup  
+30 minutes in large group discussion  
90 Minutes total

### Exercise:

1. Define alternative insider actions and strategies that could be used at each step in the scenario
2. Describe existing protection measures that could detect adversary for each step in the scenario
3. Estimate probability of detection (Pd) and probability of correct assessment (Pa) for each step (H, M, or L)
4. Identify the best insider strategy for each step in the scenario
5. Describe the optimal scenario

### Report Your Results in Large Group Discussion:

Each subgroup will present their scenario to the class for input and discussion.





# Exercise 13

## Protracted Theft

---

### Session Objectives:

After the session the participants will be able to do the following:

1. Each group will be able to identify steps in potential protracted theft scenarios for the Uranium Research Facility (URF).
2. Identify physical protection (PP), material control (MC) and material accounting (MA) measures that protect against the scenarios.
3. Identify methods the adversary could use to covertly or overtly reduce the effectiveness of these measures.
4. Estimate the effectiveness of these measures.
5. Estimate the risk associated with the scenarios.

### Estimated Time:

60 minutes in subgroup  
+30 minutes in large group discussion  
90 Minutes total

### Part A – Discrete Items:

1. Define scenarios - develop protracted theft scenarios components.
  - a. Choose two target locations with materials in discrete item form (e.g., cans of chips in charge makeup area or of oxide in bunker)
  - b. Choose two insider types
  - c. Three alternative acquisition strategies (number of acquisitions, mass, timing)
  - d. Two MAA removal strategies
  - e. Two PA removal strategies
2. Pre-screen scenarios - Discuss effectiveness of each of the  $2 \times 2 \times 3 \times 2 \times 2 = 48$  scenarios and choose two scenarios for quantitative analysis
3. Assess effectiveness of PP, MC and MA measures for each action, by each adversary type in each of the two scenarios
  - a. Probability of detection during acquisition (Pda)
  - b. Probability of detection by material accounting system (Pd(t))
  - c. Probability of detection during exit from Protected Area (Pe)
  - d. Overall probability of detection for each scenario

4. Discuss potential facility upgrades (physical and procedural) that could reduce risk

## **Part B – Bulk Materials:**

1. Define scenarios - develop protracted theft scenarios components.
  - a. Choose two target locations with materials in bulk form (e.g., casting furnace or chip vault)
  - b. Choose two insider types
  - c. Three alternative acquisition strategies (number of acquisitions, mass, timing)
  - d. Two MAA removal strategies
  - e. Two PA removal strategies
2. Pre-screen scenarios - Discuss effectiveness of each of the  $2 \times 2 \times 3 \times 2 \times 2 = 48$  scenarios and choose two scenarios for quantitative analysis
3. Assess effectiveness of PP, MC and MA measures for each action, by each adversary type in each of the two scenarios
  - f. Probability of detection during acquisition (Pda)
  - g. Probability of detection by material accounting system (Pd(t))
  - h. Probability of detection during exit from Protected Area (Pe)
  - i. Overall probability of detection for each scenario
4. Discuss potential facility upgrades (physical and procedural) that could reduce risk

## **Report Your Results in Large Group Discussion:**

Each subgroup will present one of their scenarios to the class for input and discussion.

**Exercise 13 – Protracted Theft**

1. Define scenarios - develop protracted theft scenarios components.
2. Pre-screen scenarios - Discuss effectiveness of each of the  $2 \times 2 \times 3 \times 2 \times 2 = 48$  scenarios and choose two scenarios for quantitative analysis

| Target location and material | Insider types | Acquisition strategies (number, mass, timing) | MAA removal strategies | PA removal strategies |
|------------------------------|---------------|---|------------------------|-----------------------|
| 1.                           | 1.            | 1.  | 1.                     | 1.                    |
| 2.                           | 2.            | 2.  | 2.                     | 2.                    |
|                              |               | 3.  |                        |                       |

| Exercise 13 - Scenario 1: Target location = |   |                  | Adversary type =    |     |       |    |
|---|---|------------------|---------------------|-----|-------|----|
|   | Step  | Strategies       | Protection elements | Pda | Pd(t) | Pe |
| 1   | Acquire targets over time and accumulate in MAA | ___ acquisitions |                     |     |       |    |
|   |   | ___ g each       |                     |     |       |    |
|   |   | ___ days each    |                     |     |       |    |
|   |   | ___ acquisitions |                     |     |       |    |
|   |   | ___ g each       |                     |     |       |    |
|   |   | ___ days each    |                     |     |       |    |
|   |   | ___ acquisitions |                     |     |       |    |
|   |   | ___ g each       |                     |     |       |    |
|   |   | ___ days each    |                     |     |       |    |
| 2   | Remove from MAA                                 |                  |                     |     |       |    |
|   |   |                  |                     |     |       |    |
| 3   | Remove from PA                                  |                  |                     |     |       |    |
|   |   |                  |                     |     |       |    |

| Exercise 13 - Scenario 2: Target location = |   |                  | Adversary type =    |     |       |    |
|---|---|------------------|---------------------|-----|-------|----|
|   | Step  | Strategies       | Protection elements | Pda | Pd(t) | Pe |
| 1   | Acquire targets over time and accumulate in MAA | ___ acquisitions |                     |     |       |    |
|   |   | ___ g each       |                     |     |       |    |
|   |   | ___ days each    |                     |     |       |    |
|   |   | ___ acquisitions |                     |     |       |    |
|   |   | ___ g each       |                     |     |       |    |
|   |   | ___ days each    |                     |     |       |    |
|   |   | ___ acquisitions |                     |     |       |    |
|   |   | ___ g each       |                     |     |       |    |
|   |   | ___ days each    |                     |     |       |    |
| 2   | Remove from MAA                                 |                  |                     |     |       |    |
|   |   |                  |                     |     |       |    |
| 3   | Remove from PA                                  |                  |                     |     |       |    |
|   |   |                  |                     |     |       |    |

# Exercise 14

## Upgrades Analysis

---

### **Session Objectives:**

After the session the participants will be able to do the following:

1. Identify system strengths and weaknesses for the spectrum of threats
2. Identify safeguards upgrades that address individual weaknesses
3. Package the alternative upgrades for meaningful analysis of their benefits
4. Estimate costs and operational impacts of these upgrades packages; rank them

### **Estimated Time:**

60 minutes in subgroup  
+30 minutes in large group discussion  
90 Minutes total

### **Exercise:**

1. Identify key weaknesses in the protection system
2. Develop a list of potential upgrades that could address each weakness
3. Estimate the effectiveness of each upgrade (increase in Pd or Pa)
4. Estimate the life cycle cost of each upgrade (\$)
5. Form effectiveness/benefit ratio of each upgrade and identify the best ones

### **Report Your Results in Large Group Discussion:**

Each subgroup will present their scenario to the class for input and discussion.